1 April 2026

Our reference: BOSE-2026-101

Epic Games Entertainment International GmbH

c/o s 47F

Platz 10, 6039 Root D4, Switzerland

By email: s 47G(1)(a) @epicgames.com

Dear s 47F

Non-periodic reporting notice requiring Epic Games Entertainment International GmbH to prepare a report about the extent to which it has complied with the Basic Online Safety Expectations

The eSafety Commissioner is responsible for improving and promoting online safety for Australians. This includes giving notices to service providers about their compliance with the Basic Online Safety Expectations ('the Expectations'), and publishing summaries of our findings. For more information about eSafety's role and functions, please refer to our website.

The publication of findings serves to increase the transparency and accountability of online services in demonstrating the actions that they are taking to protect Australians from harms online. Transparency also empowers Australians with information to better understand the online environment and any safety risks that may be present on services.

By highlighting what we have learned from notices, eSafety's aim is that the information is also used by researchers, academics, the media and the public to scrutinise the efforts of industry to encourage implementation of the Expectations and to lift safety practices, protections and standards across the industry.

Please see enclosed a non-periodic reporting notice (**the Notice**) given to Epic Games Entertainment International GmbH (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**). The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Basic Online Safety Expectations during the period specified in the Notice in respect to the Fortnite service (the **Service**).

The Notice requires the Provider to give the report to the Commissioner by **17:00 Australian Eastern Standard Time (AEST) on 18 May 2026.**

If you require additional time to comply with the Notice, you may request this by sending an email to industryBOSE@esafety.gov.au before **17:00 AEST on 4 May 2026.**

The manner and form of the required report are included in **Schedule B** to the Notice. Instructions on this requirement are included in the Notice. Definitions of relevant terms are included in **Schedule C** to the Notice.

The specified applicable Basic Online Safety Expectations

The Notice focuses on the steps being taken to comply with the Expectations, with a focus on unlawful and/or harmful material and activity which:

a. is child sexual exploitation and abuse (CSEA);

b. promotes, incites or instructs in matters of violence;

c. is cyber-bullying; and

d. falls under Provider's community rules on 'Intolerance and Discrimination[1],[2] content guidelines on 'Discriminatory Content' or Fortnite Developer rules on 'Intolerance and Discrimination[3].

The Expectations are contained in the Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) (the **Determination**), which commenced on 24 January 2022. The relevant regulatory guidance is available here.

What you are required to report on

See **Schedule A** for full details of the specific expectations that, under the Notice, the Provider is required to report on.

The decision to give the Notice

I have decided to give the Notice under section 56(2) of the Act. In deciding whether to give a non-periodic reporting notice, I am required by section 56(5) of the Act to have regard to the following criteria, against which I have summarised my considerations:

a) The number of occasions during the previous 12 months on which complaints about material provided on the Service were made to the Commissioner under the Act:
   - During the period 20 March 2025 to 20 March 2026, the eSafety Investigations Branch received 10 complaints relating to material available on the Service, including 4 complaints relating to cyberbullying material; 1 relating to Imaged based abuse; and 3 relating to illegal and restricted content.
   - I do not rely on this factor as a reason for giving this Notice.

b) Whether the provider has previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act:
   - The Provider has not previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act. I do not rely on this factor as a reason for giving this Notice.

c) Whether there are deficiencies in the Provider's practices, so far as they relate to the capacity of end-users to use the Service in a safe manner:

[1] Epic Games, 'Epic Games Community Guidelines', accessed 30 January 2026, URL: Epic Games Community Rules - Epic Games.
[2] Epic Games, 'Epic Games – Content Guidelines', accessed 30 January 2026, URL: Epic Games Content Guidelines - Epic Games.
[3] Epic Games, 'Fortnite Developer Rules;, accessed 2 February 2026, URL: https://legal.epicgames.com/en-US/fortnite/developer-rules

- I note reports from expert agencies, research and media reports relating to the potential for unlawful and/or harmful material or activity, as well as harms associated with online gaming services, particularly as they relate to children.

- I consider that these reports indicate a risk that Australians, especially Australian children, may be exposed to unlawful or harmful material or activity on the Service. The Notice would assist me in understanding what steps the Provider is taking to comply with Expectations 6(2) and 6(2A).

a) Whether there are deficiencies in the Service's terms of use, so far as they relate to the capacity of end-users to use the Service in a safe manner:
    - I consider the Notice would assist me in understanding the steps the Provider is taking to enforce its terms of service and comply with Expectation 14(1A) of the Determination.

b) Whether the Provider has agreed to give the Secretary regular reports relating to the capacity of end-users to use the Service in a safe manner;
    - There is no ongoing agreement between the Provider and the Secretary of the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts for regular reports for the purpose of section 56(5)(e). As such, I consider the Notice to be of assistance to exercising my statutory functions.

c) Such other matters (if any) as the Commissioner considers relevant.
    - As well as the considerations above:
        - I consider the use of the Service by Australians to be a risk factor as any failure to comply with the relevant Basic Online Safety Expectations puts Australians at risk, including children.
        - I consider that the Service's features, such as its chat functions which enable interaction between children and adults; its ability to create user-generated content; its immersive features; and its use of in-app currency are features with the potential to increase the risk of CSEA activity (e.g. grooming and sexual extortion) and violence material and activity (e.g. youth radicalisation) if appropriate safeguards are not put in place by the Provider.
        - I consider that the following information gaps limit eSafety's understanding of the steps the Provider is taking to ensure safe use and proactively minimise harmful content such as CSEA, violence material and cyberbullying on the Service, including:
            - Quality of training data and effectiveness of moderation tools;
            - Information on content moderators;
            - Information sharing with other providers;
            - Measures to address recidivism.

Additionally, giving the Notice supports my statutory functions as set out in section 27 of the Act, including to promote online safety for Australians, to monitor compliance with the Act, and to collect, analyse, interpret and disseminate information relating to online safety for Australians.

Required action

The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Expectations during the period specified in the Notice and give the report to the Commissioner by **17:00 AEST on 18 May 2026.**

Failure to comply with the Notice may result in the Commissioner taking enforcement action.

You should contact eSafety prior to the Notice deadline if any of the following apply, and take the steps indicated:

- You consider that a question does not apply to your Service. Provide reasons and an explanation of why the question does not apply.
- You consider that you are not capable of answering a question. Identify the question(s) and provide reasons and an explanation of why you are not capable of answering the question(s). eSafety will consider your reasons and explanation and advise on an appropriate course of action.
- You require additional time to comply with the Notice and to provide the required information. You must request an extension of time from eSafety and provide specific reasons why you are not capable of meeting the deadline specified in the Notice. eSafety will inform you if an extension of time has been granted by the Commissioner.
- You would like to request an alternative means of returning Schedule B to the Notice other than via Qualtrics. Provide reasons and suggest an alternative method of providing the information. eSafety will arrange appropriate alternate means where appropriate.

eSafety will engage with all providers who contact eSafety. We request that you comply with the instructions given by eSafety in response to any of the above requests.

Extension of time to comply

If the Provider requires additional time to comply with the Notice, please email industryBOSE@esafety.gov.au before **17:00 AEST on 4 May 2026.** In your email, please include reasons for your request.

You may seek an extension of time any time before **17:00 AEST on 4 May 2026**. If you submit a request for an extension of time less than 2 weeks prior to **17:00 AEST on 18 May 2026**, you should include reasons as to why an extension was not sought earlier, as well as reasons for the request.

The deadline in the Notice continues to apply unless eSafety confirms that an extension is granted.

Failure to comply

Under section 57 of the Act, the Provider must comply with the requirement under the Notice to the extent that it is capable of doing so.

Failure to comply with the Notice is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate, following the end of the period specified for compliance with the Notice. eSafety also has a range of other enforcement options, as detailed in the regulatory guidance.

False or misleading information or documents

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to eSafety or the eSafety Commissioner.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Review rights

The Provider has a right to seek an internal or external review of the decision to give a notice to it under section 56(2) of the Act.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

More detailed information about the Provider's review rights is available in the information sheet at Schedule D to this correspondence which sets out the Provider's rights with respect to the different review options available to it, as well as other options if you do not agree with the decision to give the Notice to the Provider.

Confidentiality

eSafety intends to publish a summary of the Provider's responses to the Notice, pursuant to section 217 of the Act. Part of the purpose of collecting the information required under the Notice is publication of that information.

The Provider can make submissions about confidentiality and/or the sensitivity of information provided to eSafety. eSafety will carefully consider any objections when deciding what information to publish. Attachment A to this correspondence outlines the criteria that eSafety will have regard to in considering confidentiality submissions.

The Provider must provide the information required by the Notice even if you have concerns about confidentiality and/or sensitivity of certain information and make submissions to eSafety about the publication of confidential and sensitive information.

eSafety will prepare a summary of information for publication. Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, the Provider will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.

Regards,



Julie Inman Grant
eSafety Commissioner

Enclosed: Notice under section 56(2) of the Act

Information Sheet: Review Rights

NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Epic Games Entertainment International GmbH (the **Provider**)

Attention: s 47F

Epic Games Entertainment International GmbH, Platz 10, 6039 Root D4, Switzerland

By Email: s 47G(1)(a) **@epicgames.com**

This non-periodic reporting notice (**Notice**) is given to Epic Games Entertainment International GmbH (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) in respect of the Fortnite service (the **Service**) that it provides in Australia.

The Provider is required to prepare a report about the extent to which it complied with the applicable Basic Online Safety Expectations specified in **Schedule A** for the period 1 October 2025 to 31 March 2026 inclusive (**Report Period**).

The Provider is required to provide the report in the manner and form specified in **Schedule B,** including following the instructions provided, and answering the questions included in **Schedule B.**

The Provider is required to give the report to the Commissioner within 47 days of being given this Notice, being no later than **17:00 AEST on 18 May 2026** (the **Due Date**), or within such longer period as the Commissioner allows if the Commissioner is contacted by the Provider with a request for an extension of time.

The report is to be submitted to the Commissioner via the Qualtrics report form in Schedule B of the Notice.

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate.

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Date: 1 April 2026

Julie Inman Grant

eSafety Commissioner

Schedule A – specified applicable Basic Online Safety Expectations

The Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) (**Determination**) commenced on 24 January 2022 and contains the Basic Online Safety Expectations, some of which Epic Games Entertainment International GmbH (the **Provider**) as the provider of the Fortnite service (the **Service**), is being required to report on under this Notice. The amendments to the Determination made by the Online Safety (Basic Online Safety Expectations) Amendment Determination 2024 (Cth) came into effect on 31 May 2024.

This Schedule sets out the specified applicable Basic Online Safety Expectations to be reported on by the Provider for the purpose of this Notice:

Expectations:

6 Expectations—provider will take reasonable steps to ensure safe use

Additional expectation

(2) The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful.

Additional expectation

(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

10 Additional expectation—provider will consult and cooperate with other service providers to promote safe use

Additional expectation

(1) The provider of the service will take reasonable steps to:

(a) consult and cooperate with providers of other services; and

(b) ensure consultation and cooperation occurs between all relevant services provided by that provider, in order to promote the ability of end-users to use all of those services in a safe manner.

11 Core expectation—provider will take reasonable steps to minimise provision of certain material

The provider of the service will take reasonable steps to minimise the extent to which the following material is provided on the service:

(a) cyber-bullying material targeted at an Australian child;

(b) cyber-abuse material targeted at an Australian adult;

(c) a non-consensual intimate image of a person;

(d) class 1 material;

(e) material that promotes abhorrent violent conduct;

(f) material that incites abhorrent violent conduct;

(g) material that instructs in abhorrent violent conduct;

(h) material that depicts abhorrent violent conduct.

12 Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

Core expectation

(1) The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

14 Additional expectations—provider will ensure service has terms of use, certain policies etc.

(1A) The provider of the service will take reasonable steps (including proactive steps) to detect breaches of its terms of use and, where applicable, breaches of policies and procedures in relation to the safety of end-users, and standards of conduct for end-users.

(2) The provider of the service will take reasonable steps (including proactive steps) to ensure that any penalties specified for breaches of its terms of use, policies and procedures in relation to the safety of end-users, and standards of conduct for end-users, are enforced against all accounts held or created by the end-user who breached the terms of use and, where applicable, breached the policies and procedures, and standards of conduct, of the service.

Schedule B – Qualtrics report form[4]

This report form constitutes Schedule B to the Notice. It specifies the manner and form of the report required by the Notice and requires you to respond to the questions included within, which relate to the Provider's compliance with the applicable Basic Online Safety Expectations. The relevant expectations are stated alongside each question.

Each of the following is a requirement under the Notice:

- Answer each question truthfully and accurately. Other information provided to the eSafety Commissioner ('eSafety') in relation to the Notice, including statements about a provider's capability to respond to the Notice and submissions related to confidentiality or sensitivity of information, must also be truthful and accurate.
- Use this report form for your response. Responding in an alternative way without prior agreement with eSafety may amount to non-compliance with the Notice.
- Provide a response to each question, and its parts unless the report form states otherwise. Leaving a response blank without providing eSafety with a reasonable explanation in advance of the deadline for the Notice (or any valid extension of time) is likely to be considered as non-compliance with the Notice.
- Provide information for the period from 1 October 2025 to 31 March 2026 (**the Report Period**), unless a question requires information on a specific time period within the Report Period. Some questions may require information as at a specified date. The use of this date within the Report Period ensures that eSafety can obtain up to date information on providers' current practices and aims to reduce the burden on providers.

Navigating through the report form:

- The report form includes single and multiple response options as well as text field options.
- All text fields allow for the available window space to be increased by clicking and dragging the right bottom corner of the box and re-sizing as required.
- A Table of Contents is provided at the top left-hand side to allow for easy navigation though the questions. The forward and back buttons will allow for navigation to any question.
- A response to a question may result in subsequent questions no longer requiring a response. All questions to the report form are displayed, regardless of whether a response is required. This is to provide transparency of the full set of questions.
- Some questions are Provider specific and where there is a question for a different Provider, a note is included to note that the question has been skipped.

---

[4] Link to Qualtrics report form – https://esafetydxm.qualtrics.com/jfe/form/SV_9traCr0DRCfIGKW?Q_CHL=gl&Q_DL=EMD_3dsuwk80bOEmzg4_9traCr0DRCfIGKW_CGC_E5sM9G5KxIk4OoR&_g_=g

- Responses are automatically saved in draft and can be revisited over the course of multiple sittings.
- Before submitting the responses, you are required to review all questions to ensure responses are provided.
- Once the report form is submitted, no further changes can be made. You may contact eSafety to reopen a submitted response before the Due Date.
- Once responses are submitted there will be a summary page with an option to download a copy of your responses to a PDF document.

Also note the following:

- Include as much information as is necessary to provide a fulsome response to the question. Question 78 is an opportunity for you to provide information as part of your report about any further safety measures the Provider is taking to comply with these specified expectations.
- You can raise concerns about confidentiality and/or the sensitivity of information. eSafety will carefully consider your submissions when deciding what information to publish. **Attachment A** has been provided to you to outline the criteria that eSafety will have regard to in considering confidentiality submissions. However, concerns about the confidentiality and sensitivity of certain information are not adequate reasons to refuse to provide information required by the Notice. eSafety will prepare a summary of information for publication based on the Provider's responses.
- Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, you will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.
- **Definitions of relevant terms are included in Schedule C to the Notice.** If you have any concerns about the relevant terms, contact us at industryBOSE@safety.gov.au to discuss.
- Further information can also be found in the Basic Online Safety Expectations Regulatory Guidance and on the relevant page on eSafety's website.
- You can contact industryBOSE@safety.gov.au regarding any of the above information, or with any other questions about your response.
- On the final page where the 'submit' button is displayed, the following text will be included:

  This is the final page of Schedule B to the Notice. Please review your responses. Once you click 'submit', your response will be received by eSafety and all information provided is considered [Provider]'s response to the Notice. Note that you cannot edit your response after you click 'submit'.

Schedule C – Definitions of relevant terms

The Act: *The Online Safety Act 2021* (Cth).

Age assurance: An umbrella term which includes age verification (determining a person's age to a high level of accuracy, such as through the use of identity documents)l age estimation (providing an approximate age through analysis of biological or behavioural human features that vary with age, for example through the use of facial or voice analysis), or age inference (using information other than a date of birth which indirectly implies a certain age or age range).

Child sexual exploitation and abuse (CSEA): Material or activity which includes both:

- 'child sexual exploitation' (a broad category that encompasses material and activity that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse)
- 'child sexual abuse' (which involves a sexual assault against a child, is a narrower category and can be considered a sub-set of child sexual exploitation).

CSEA material is a subset of class 1 material, as defined under section 106 of the Act by reference to the National Classification Scheme, and includes images video and text. CSEA material includes user generated content.

CSEA activity refers to other illegal activity, including grooming and sexual extortion of children. CSEA activity can include attempts to migrate children to a third party service for the purpose of grooming or sexually extorting a child.

See also the definitions in the Industry standards for Relevant Electronic Services regarding class 1A and class 1B material: Register of industry codes and industry standards for online safety | eSafety Commissioner

Class 1 material: Material that is, or would likely be, refused classification (**Refused Classification or RC**) by the Classification Board under the National Classification Scheme. It includes material that: '

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence, or
- advocates the doing of a terrorist act.

Class 2 material: Material that is, or would likely be, classified R 18+ or X 18+ under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old (such as pornography, and other high impact material).

Cyberbullying material targeted at an Australian child: Has the meaning given at section 6 of the Online Safety Act 2021.

End-user: A natural person who is an end-user of a product or online service.[5]

Grooming: The process of building an emotional connection with a child in order to sexually abuse or exploit them. This increasingly involves children being tricked or coerced into sexual activity on webcams or into sending sexual images through online services. Grooming is a type of CSEA activity.

Hash-matching tools: Digital technology used to create a unique digital signature (known as a 'hash') of an image or video which is then compared against signatures (hashes) of other photos to find copies of the same image or video.

Hash database: A database of material that has been previously confirmed to contain harmful and/or unlawful material. For example, the Global Internet Forum to Counter Terrorism hash-sharing database.

Language analysis tools: Technologies using methods to assign a probability that text or conversations involve certain behaviour, such as grooming a child for sexual abuse. This may involve artificial intelligence programming.

Material: Defined in section 5 of the Act to mean material, whether in the form of text, data, speech, music or other sounds, visual images (moving or otherwise), of any other form or any combination of forms. In the context of CSEA, 'material' typically refers primarily to images or video content.

Notice: A non-periodic notice given to a provider under section 56(2) of the Act on 1 April 2026.

Online hate policies: Policies relating to the Provider's Community Rules on 'Intolerance and Discrimination',[6] Content Guidelines on 'Discriminatory Content'[7] and Fortnite Developer Rules on 'Intolerance and Discrimination'.[8]

Recidivism: In the context of this Notice, banned or suspended users re-registering to a service with the same or new details. Multiple fake or imposter accounts may be created by a human user or by an automated bot programmed by a human.

Report period: When providers receive a reporting Notice from the eSafety Commissioner ('eSafety') they are required to prepare a report about the extent to which they complied with the Expectations during a specified period. This period is referred to as the 'report period'. The report period for this set

---

[5] 'Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms', 2025, accessed 18 August 2025, URL: https://onlinesafety.org.au/wp-content/uploads/2025/07/CLEAN-Phase-2-OSA-Codes-Head-Terms-1.pdf

[6] Epic Games, 'Epic Games Community Guidelines', accessed 30 January 2026, URL: Epic Games Community Rules - Epic Games.

[7] Epic Games, 'Epic Games – Content Guidelines', accessed 30 January 2026, URL: Epic Games Content Guidelines - Epic Games.

[8] Epic Games, 'Fortnite Developer Rules;, accessed 2 February 2026, URL: https://legal.epicgames.com/en-US/fortnite/developer-rules

of Notices is 1 October 2025 to 31 March 2026. Information provided reflects this period, unless stated otherwise.

Sexual extortion: A crime involving online blackmail, where victims are tricked into sending intimate images of themselves to someone who then threatens to share the images unless demands are met, usually for payment. eSafety requires information relating to any instance of sexual extortion, not only those including children. Sexual extortion is a type of CSEA activity.

Violence material and activity: Material or activity which promotes, incites or instructs in matters of crime or violence. Violence material is material which would be, or would likely be, defined as class 2 material for the purposes of section 107 of the Act, or class 1 material for the purposes of section 106 of the Act.

Violence material includes pro-terror material, crime and violence material and extreme crime and violence material as define by the Industry Standards for Relevant Electronic Services: Register of industry codes and industry standards for online safety | eSafety Commissioner. For the purposes of this notice, violence activity may include attempts to migrate children to an external platform for the purposes of sharing violence material (e.g. sharing links to a specific forum or community associated with violence material or activity).

Schedule D - Information sheet: Right of Review

Internal review by the eSafety Commissioner (eSafety)

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things:

- affirm the eSafety Commissioner's decision
- vary the eSafety Commissioner's decision; or
- set the eSafety Commissioner's decision aside and replace it with its own decision.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be waived, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

If we have not provided the reasons for this decision, you may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by eSafety under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to eSafety in writing through one of the following options:

Online: using the **Contact Us** form on eSafety's website

Email: FOI@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal or email address for us to reply to and which we can use to communicate with you about your application.

eSafety's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that eSafety has handled this matter, we ask that you contact us using the **Contact Us** form on eSafety's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with eSafety first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Unlawful and/or harmful material and activity

1. Q1. Does Epic Games consider the following material and activity types to be unlawful and/or harmful?

	Choose all that apply
CSEA material and activity	☐
Violence material and activity	☐
Cyberbullying	☐
Material and activity covered by Epic Games's online hate policies	☐

Section 1: Age assurance

Expectations 6(2), 6(2A), 11 and 12.

2. Q2. During the report period, did Epic Games use tools and techniques to assess the age of end-users on Fortnite?

    a. Yes
    b. No

If yes (a) at Q2

3. Q3. Name all the tools and techniques Epic Games used to assess the age of end-users on Fortnite and whether the tool or technique was an internal proprietary tool or technique, or provided by a third party.

Name of tool or technology	Internal proprietary tool or technique	Third party tool or technique
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o

If yes to third party tool at Q3

4. Q4. For each third-party tool or technique identified at Q3, specify the name of the third-party provider.

Name of tool/technology	Third party tool provider name
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	

5. Q5. For each tool listed at Q3, specify the type of tool or technique from the list below.

Name of tool/technology	Type of technology or technique used (Drop down list will be displayed with options listed below,)
(Tool from Q3 will be auto populated)	- Self declaration - Facial age estimation - ID document verification (government) - ID document verification (non government) - Credit card verification - Age inference model - Age key - Vouching (parental) - Vouching (other user or institution) - Other
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above

If Other (specify) at Q5 – (only tools where other specify were chose will appear)

6. Q5-1. Specify the 'other' type of tool or technique used.

Name of tool	Specify the type of technology used
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	

If using Age inference models at Q5.

7. Q6. For the age inference models listed in Q5, specify all the indicators that Epic Games used to assess the age of end users on Fortnite. (multiple response)

	Choose all that apply
Operating system indicators	☐
App store indicators	☐
Cross platform indicators	☐
Language analysis	☐
Voice analysis	☐
Image classifiers	☐
Video classifiers	☐
Device identifiers	☐
IP address indicators	☐
Traffic indicators	☐
Financial indictors	☐
Behavioural indicators (list the behavioural indicators)	☐

Other (specify)	☐
Other (specify)	☐
Other (specify)	☐

If yes (a) at Q2

8. Q7. Specify when each of the tools and techniques listed in response to Q3 were used:

	At sign up	Upon accessing certain game features or parts (eg. text chat, store or particular rooms or areas within a game)	During gameplay	To access certain Islands	When an account has been flagged for review by automated tools/human moderators	In response to a user report	When the service is accessed on a particular device (e.g. console, PC, mobile)	To gain access to parental controls	Other
Name of tool from Q3 will be auto populated)	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐

If *Upon accessing certain game features (e.g. text chat, store)* at Q7 was chosen – (Only tools where this option was chosen will appear)

9. Q7-1. Specify the 'certain game features or parts (e.g. text, chat, store or particular rooms or areas within a game)' on Fortnite where the tool or technique was used.

Name of tool	Game features tool was used in
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

If other (specify) was chosen for any response at Q7

10. Q7-2. Specify when the 'other' tool or technique was used on Fortnite.

Name of tool	Specify
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	

If used a tool to assess the age of end-users (Yes at Q2)

11. Q8. During the report period, did Epic Games or a third-party provider of a tool or technique assess the effectiveness of these tools and techniques used on Fortnite?

Name of tool/technology	Yes – Epic Games assessed	Yes – Third-party provider assessed	No
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o

If yes at Q8 (assessed accuracy of the tools)

12. Q9. What metrics did Epic Games (or the third-party provider of a tool or technique) use to assess the effectiveness of each tool and technique? Include the specific metrics, and any relevant standards or certification schemes that Epic Games relied on to evaluate the effectiveness of a tool in your answer.

Name of tool/technology	Specify the effectiveness metric used for the assessment
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

13. Q10. What was the result of the assessment for effectiveness of each tool and technique?

Name of tool/technology	Specify details of the result
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

14. Q11. What action was taken as a result of the assessment for each tool and technique?

Name of tool/technology	Specify the action taken
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

15. Q12. During the report period, what action did Epic Games take after it became aware that the age information it held about an end-user may be incorrect.

	Choose all that apply
Banned account	☐
Suspended account	☐
Directed to undergo age assurance	☐
Strike against account	☐
Other (specify)	☐

IF yes at Q2

16. Q13. During the report period, specify how many end-users were found to be incorrectly age assured by the tools and techniques identified at Q3 to assess the age of end-users.

16. Q14. Provide any other relevant information or context in relation to your responses to questions 1 to 13, including:
    a. whether Epic Games undertook any research or development work during the report period in relation to age assurance
    b. whether responses to these questions are affected by whether an end-user uses Fortnite on particular devices (e.g. on a particular console, PC, or mobile)

Section 2: Staffing / Moderation

Expectations 6(2), 6(2A), 11 and 12.

17. Q15. As at 31 March 2026, provide the number of staff employed by Epic Games for the below categories.

	Specify number employed
Engineers employed by Epic Games who spend at least 50% of their time on trust and safety	
Content moderators employed by Epic Games	
Content moderators contracted employed by Epic Games	
Trust and safety staff employed by Epic Games (other than engineers and content moderators)	

18. Q16. As at 31 March 2026, provide the number of moderators (contracted or employed by Epic Games) trained in the following unlawful or harmful material or activity:

	Specify number of moderators trained in each following unlawful or harmful material or activity
Grooming	
Other CSEA material and activity	
Sexual extortion	
Violence material and activity	

19. Q17. As at 31 March 2026, specify which of the below languages Epic Games's trust and safety staff operated in.

	Choose all that apply
English	☐
Mandarin	☐
Arabic	☐
Vietnamese	☐
Cantonese	☐
Punjabi	☐
Other languages	☐

If other (specify) was chosen for any response at Q17

20. Q18. What is the total number of the **other** languages that the Epic Games's contractor trust and safety staff operated in?

Number of other languages (excluding those listed at Q17)	

21. Q19. Provide any other relevant information or context in relation to your responses to questions 15 to Q18.

Section 3: User reporting

Expectations 14(1A).

22. Q20 During the report period, specify the number of **global** end-user reports of unlawful or harmful material or activity on Fortnite which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Number of **global** end-user reports
Grooming	
Sexual extortion	
Other CSEA material) and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Epic Games's online hate policies	

23. Q21. During the report period, specify the number of **Australian** end-user reports of unlawful or harmful material or activity on Fortnite which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Number of **Australian** end-user reports
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Epic Games's online hate policies	

24. Q22. During the report period, specify the median time taken to reach an outcome after an end-user made a report, where reports were reviewed by human moderators. Provide responses for the median time concerning each of the following unlawful or harmful material or activity on Fortnite.

This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review.

Provide a response in minutes

	Median time taken (minutes)
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Epic Games's online hate policies	

25. Q23. During the report period, specify the median time taken to reach an outcome after automated tools flagged potential unlawful or harmful material or activity on Fortnite, where flags were reviewed by human moderators. Specify for each of the following unlawful or harmful material or activity.

    This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review

	Median time taken
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Epic Games's online hate policies	

26. Q24. During the report period, specify the proportion in percentage of unlawful or harmful material or activity that was detected proactively vs reported by users on Fortnite, concerning the following unlawful or harmful material or activity.

	Detected proactively (%)	Reported by end-users (%)
Grooming		
Sexual extortion		
Other CSEA material and activity		
Violence material and activity		
Cyber-bullying		
Material and activity covered by Epic Games's online hate policies		

27. Q25. Explain how the answers to questions Q20 to Q24 were calculated and provide any other context.

	Specify how answers were calculated and provide any other context
Number of **Global** end-user reports	
Number of **Australian** end-user reports	
Median time taken to reach outcome from **Global** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from **Australian** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from automated tools that were reviewed by human moderators	
Percentage of unlawful or harmful material or activity detected proactively vs reported by users	

Section 4: Action taken against end-users

Expectations 14(1A) and 14(2)

28. Q26. During the report period, what action did Epic Games take after an end-user breached the terms of service and/or community guidelines (or equivalent) in relation to the following unlawful or harmful material or activity.

	Sexual extortion	Grooming	Other CSEA material and activity		Violence material and activity	Cyberbullying	Conduct that breaches Epic Games's online hate policies
Banned account	☐	☐	☐		☐	☐	☐
Suspended account	☐	☐	☐		☐	☐	☐
Strike/Warning given to end-user	☐	☐	☐		☐	☐	☐
Restricted player's access to certain features of the game (e.g. ability to interact with other players)	☐	☐	☐		☐	☐	☐
Removed harmful content created by user (e.g. user-generated content, messages)	☐	☐	☐		☐	☐	☐
Prevented user from creating certain content (e.g. marketplace items)	☐	☐	☐		☐	☐	☐
Other (specify)	☐		☐	☐	☐	☐	☐

29. Q27. During the report period, were Epic Games's trust and safety staff automatically informed when developers banned an account from a Community for behaviour related to the following unlawful or harmful material or activity.

	Yes	No
Grooming	○	○
Sexual extortion	○	○
Other CSEA material and activity	○	○
Violence material and activity	○	○
Material and activity covered by Epic Games's online hate policies	○	○

If trust and safety were not informed automatically at Q27 – No to at least 1.

30. Q28. How did Epic Games ensure that a user banned from a Community for breaches related to the unlawful or harmful material or activity at Q27 was not able to engage in this activity on other parts of the service?

31. Q29. Provide any other relevant information or context in relation to your responses to questions 26 to 28, including whether responses to these questions are affected by whether an end-user uses a particular edition/model of Fortnite or uses Fortnite on particular devices (e.g. on a particular console, PC, or mobile)

Section 5: Tools and Techniques

Expectations 6(2), 6(2A), 11 and 12.

32. Q30. During the report period, did Epic Games use tools and/or techniques on Fortnite to detect the following unlawful or harmful material or activity?

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Other CSEA material and activity	o	o
Violence material and activity	o	o
Attempts to migrate children to another service	o	o

If used tool/techniques to identify harms (Yes for any at Q30)

33. Q31. Name all the tools and techniques used and which harm types they cover.

	Grooming [IF yes to Grooming at Q29]	Sexual extortion [IF yes to Sexual extortion at Q29]	Other CSEA material and activity [IF yes to Other CSEA at Q29]	Violence material and activity [IF yes to Violence at Q29]	Attempts to migrate children to another service [IF yes to attempts to migrate at Q29]
Tool 1 (Specify)	☐	☐	☐	☐	☐
Tool 2 (Specify)	☐	☐	☐	☐	☐
Tool 3 (Specify)	☐	☐	☐	☐	☐
Tool 4 (Specify)	☐	☐	☐	☐	☐

Tool 5 (Specify)	☐	☐	☐	☐	☐
Tool 6 (Specify)	☐	☐	☐	☐	☐
Tool 7 (Specify)	☐	☐	☐	☐	☐
Tool 8 (Specify)	☐	☐	☐	☐	☐
Tool 9 (Specify)	☐	☐	☐	☐	☐
Tool 10 (Specify)	☐	☐	☐	☐	☐

If used tool/techniques to identify violence material or violence activity at Q31

34. Q32. Specify the types of 'violence material and/or activity' the tool/technique is used to identify.

	Specify below
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	

If used tool/techniques to identify harms (Yes for any at Q30)

35. Q33. For each tool and technique identified at Q31, specify which part of the service it is used on.

[Fortnite response options]	Party text chat	Game text chat	Direct messages	Groups	Voice chat	Fortnite Community posts	Interactions between avatars	Islands	Cosmetic items (e.g. outfits, emotes)	Other (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

IF other at Q33

36. Q33-1. Specify the 'other' part of the service where the tool or technique was used.

	Specify
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

36. Q34. For each tool and technique identified at Q31, specify the type of tool or technique.

	Language analysis tool (text) `	Language analysis tool (audio)	AI classifier	Hash-matching tool	Signals-based detection (e.g. behavioural indicators, financial indicators (specify)	Other (e.g. detecting URL join links) (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐

If Other (specify) chosen for any tool at Q34.

37. Q34-1. Specify the other type of tool or technique for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

(Tool from Q34 will be auto populated if Other (specify) was chosen)	

If Signals-based detection (specify) chosen for any tool at Q34.

38. Q35. Specify the signals used for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

39. Q36. For each tool or technique identified Q31, specify whether the tool detects material before or after it is published (i.e. as part of a pre-screening process).

	Before material is published	After material is published	Provide any relevant details
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	

If used hash-matching tool at Q34

40. Q37. For each hash-matching tool identified at Q34, specify the names of the hash-matching source databases used.

Choose all that apply.

	GIFCT	IWF	NCMEC	Other (specify)
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	

Q37-1. Please specify the 'other' hash-matching source database for the tools below.

	Other (specify)
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

41. Q38. For each hash-matching tool identified at Q34, specify the frequency at which Epic Games updated the hashes it scanned on Fortnite against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (Specify)
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○

41. Q38-1. Specify the 'other' frequency at which Epic Games updated the hashes it scanned on Fortnite against these databases.

	Specify
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

IF used language analysis tool at Q34

42. Q39. For each language analysis tool identified at Q34, specify all the languages it operated in.

Choose all that apply.

	English	Mandarin	Arabic	Vietnamese	Cantonese	Punjabi	Other	Language agnostic
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐

If other (specify) was chosen for any response at Q39

43. Q40. What is the total number of **other** languages that the language analysis tool operated in?

Number of other languages (excluding those listed at Q39)	

If use language analysis tool at Q34

44. Q41. For each language analysis tool identified at Q34, specify whether the tool has been trained to do any of the following:

	Key-word detection	Interpret sentence	Interpret conversat	Distinguish joking/ir	Interpret coded or indirect	Interpret formatting or	Detect coercive or	Detect attempts to	Provide any other

		level context	ion-level context	ony from serious intent	language (includin g use of emojis or symbols in words)	hashtags as context clues	manipula tive language	migrate children to another service	relevant details
(Languag e analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Languag e analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Languag e analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Languag e analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Languag e analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	

If tool used language analysis tools at Q34

45. Q42. List all the organisations used to source keywords/training data for the language analysis tools listed below.

	GIFCT	IWF	NCMEC	Lantern	Other (specify)
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	

IF other at Q42

45. Q42-1. Provide details on the other organisations used to source keyword/training data for the language analysis tools.

	Other (specify)
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	

If tool used language analysis tools at Q34

46. Q43. For each language analysis tool identified at Q34, specify the frequency Epic Games updated the tool against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (specify)
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○

IF other at Q43

46. Q43-1. Provide details on the frequency that Epic Games updated the language analysis tools against the source keyword/training data.

47. ASK ALL who use tools Q33 yesQ44. During the report period, did Epic Games assess the accuracy of all the below tools used to detect the unlawful or harmful material or activity?

	Yes	No
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o

If assessed accuracy of tools (Yes at Q44)

48. Q45. Provide details of the assessment methodology, specify details of any red teaming or simulated adversarial testing.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

49. Q46. What were the results of this assessment? Include **precision** and **recall rates** in your answer, and/or **any other metrics used to quantify the result**, with relevant context.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

50. Q47. What action was taken as a result of the assessment for each tool?

	Specify action taken
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

51. Q48. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **Grooming**?

	Used on all material by default	Used on material in some circumstances

(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Grooming at Q48.

57. Q48-1. If only in certain circumstances for Grooming, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	

53. Q49. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **sexual extortion**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for sexual extortion at Q49

57. Q49-1. If only in certain circumstances for sexual extortion, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	

54. Q50. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **other CSEA material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Other CSEA at Q50

57. Q50-1. If only in certain circumstances for other CSEA material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	

55. Q51. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **violence material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for violence material and activity at Q51

57. Q51-1. If only in certain circumstances for violence material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	

56. Q52. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances **on attempts to migrate children to another service**?

	Used on all material by default	Used on material in some circumstance
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for attempts to migrate children at Q52

57. Q52-1. If only in certain circumstances on attempts to migrate children to another service, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	

58. Q53. During the report period, did Epic Games take steps to identify Islands which may be higher risk for grooming, sexual extortion, other CSEA material and activity, violence material and activity and/or material and activity captured by [Provider's] online hate policies? Y/N

If Yes at Q53

59. Q54. Specify any measures used by Epic Games, in addition to the tools and techniques identified at Q31 to address grooming, sexual extortion, other CSEA material and activity, violence material and activity and online hate policies on these higher risk Islands.

60. Q55. During the report period, did Epic Games use any tools or other measures to detect transactions of V-Bucks and/or V-Bucks gift cards that may be linked to grooming and/or sexual extortion?

    1. Yes (specify details)
    2. No

61. Q56. Specify the details of the tools or other measures used to detect transactions of V-Bucks or V-Bucks gift cards that may be linked to grooming and/or sexual extortion.

62. Q57. Provide any other relevant information or context in relation to your responses to questions 39 to 46, including:
    a. whether Epic Games undertook any research or development work during the report period in relation to proactive detection of the harms listed in Q30
    b. whether responses to these questions are affected by whether an end-user uses Fortnite on particular devices (e.g. on a particular console, PC, or mobile)

Section 6: Recidivism

Expectations 14(1A).

63. Q58. During the report period, did Epic Games use the below indicators to identify recidivism after an end user had been banned or suspended for CSEA or violence material and activity.

	CSEA	Sexual extortion	Violence material and activity
Device identifiers	☐	☐	☐
Phone number	☐	☐	☐
Behavioural indicators	☐	☐	☐
Email address	☐	☐	☐
Geographical indicators	☐	☐	☐

Financial indicators	☐	☐	☐
Profile picture	☐	☐	☐
Username	☐	☐	☐
Name	☐	☐	☐
Date of birth	☐	☐	☐
Display name	☐	☐	☐
Other (specify)	☐	☐	☐
Other (specify)	☐	☐	☐

If used indicators to identify recidivism at Q58.

64. Q59. Were indicators used by default in all cases where an account has been banned or suspended for **CSEA material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

65. Q60. Were indicators used by default in all cases where an account has been banned or suspended for **sexual extortion**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

66. Q61. Were indicators used by default in all cases where an account has been banned or suspended for **violence material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

If used indicators to identify recidivism at Q58.

67. Q62. What specific action did Epic Games take based on these indicators? If the action taken differed based on the specific indicators, specify all those differences, e.g. automatically blocked accounts with these indicators from being created; flagged the account for human review etc.

	Specify action taken
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	

(Auto populate indicators used at Q58)	

68. Q63. Provide any other relevant information or context in relation to your responses to questions 58 to 62 including:
    a. whether Epic Games undertook any research or development work during the report period in relation to prevention of recidivism on Fortnite
    b. whether responses to these questions are affected by whether an end-user uses Fortnite on particular devices (e.g. on a particular console, PC, or mobile)

Section 7: Moderation of user-generated content

Expectations 14(1A).

NA

Section 8: Information sharing initiatives

Expectations 10(1) and 14(1A).

70. Q66. During the report period, did Epic Games share information with the following services or initiatives (including bi-lateral arrangements with other providers) for the purpose of minimising grooming/sexual extortion and violence material and activity on its service?

	Choose all that apply
Lantern	☐
Tech Coalition	☐
Fair Play Alliance	☐
Tech Against Terrorism	☐
Discord	☐
Twitch	☐
Steam	☐
Other Initiatives/Services (specify)	☐

If a member of information sharing initiative (any at Q66)

71. Q67. Explain the steps taken as a result of sharing information with the below initiatives.

	Specify steps taken
(Auto populate sharing initiative chosen at Q669)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	

(Auto populate sharing initiative chosen at Q66)	

72. Q68. Provide any other relevant information or context in relation to your responses to questions 66 to 67, including whether Epic Games undertook any research or development work during the report period in relation to collaborating with civil society organisations or other service providers to prevent harm on Fortnite

Section 9: Off-platform monitoring

Expectations 6(2), 6(2A), 11 and 12.

73. Q69. During the report period, did Epic Games use off-platform monitoring (monitoring of activity on other services either provided internally or by third-party services) to identify accounts or communities present on its service that are engaged in the below harms.

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Violence activity	o	o

If used off-platform monitoring (Yes at Q69)

74. Q70. Provide details, specifying what this involved and what third party services were used.

	Specify details	Specify names of third parties used
Grooming		
Sexual extortion		
Violence activity		

75. Q71. Provide any other relevant information or context in relation to your responses to Q69 and Q70 , including whether Epic Games undertook any research or development work during the report period in relation to monitoring of other services to identify accounts or communities engaged in the harms listed at Q69.

Section 10: Other

Expectations 6(2), 6(2A) and 11.

76. Q72. During the report period, did Epic Games provide any help services or support to users who were identified as potential victims of grooming and/or sexual extortion?
    a. Yes
    b. No

IF yes at Q72

77. Q73. Provide details on the help services or support Epic Games provided to users who were identified as potential victims of grooming and/or sexual extortion.

78. Q74. As at 31 March 2026, specify the proportion of under 18 accounts in Australia that have parental supervision enabled.

79. Q75. Explain how the answer to Q74 was calculated and provide any other context, including whether the use of parental controls on Fortnite are affected by whether an end-user uses Fortnite on particular devices (e.g. on a particular console, PC, or mobile).

Section 11: Final question

80. Q78. Outline any further steps Epic Games is taking to meet Expectations 6(2), 6(2A), 10(1), 11, 12, 14(1A) and 14(2).

    Do not replicate information provided in previous responses here. This is an opportunity for Epic Games to outline information about other types of safety measures.

1 April 2026

Our reference: BOSE-2026-102

Mojang AB

c/o s 47F, Digital Safety Unit, Microsoft

By email: s 47F @microsoft.com

Dear s 47F

Non-periodic reporting notice requiring Mojang AB to prepare a report about the extent to which it has complied with the Basic Online Safety Expectations

The eSafety Commissioner is responsible for improving and promoting online safety for Australians. This includes giving notices to service providers about their compliance with the Basic Online Safety Expectations (the **Expectations**), and publishing summaries of our findings. For more information about eSafety's role and functions, please refer to our website.

The publication of findings serves to increase the transparency and accountability of online services in demonstrating the actions that they are taking to protect Australians from harms online. Transparency also empowers Australians with information to better understand the online environment and any safety risks that may be present on services.

By highlighting what we have learned from notices, eSafety's aim is that the information is also used by researchers, academics, the media and the public to scrutinise the efforts of industry to encourage implementation of the Expectations and to lift safety practices, protections and standards across the industry.

Please see enclosed a non-periodic reporting notice (**the Notice**) given to Mojang AB (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**). The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Basic Online Safety Expectations during the period specified in the Notice in respect to the Minecraft service (the **Service**).

The Notice requires the Provider to give the report to the Commissioner by **17:00 Australian Eastern Standard Time (AEST) on 11 May 2026.**

If you require additional time to comply with the Notice, you may request this by sending an email to industryBOSE@esafety.gov.au before **17:00 AEST on 27 April 2026.**

The manner and form of the required report are included in **Schedule B** to the Notice. Instructions on this requirement are included in the Notice. Definitions of relevant terms are included in **Schedule C** to the Notice.

The specified applicable Basic Online Safety Expectations

The Notice focuses on the steps being taken to comply with the Expectations, with a focus on the following unlawful and/or harmful material and activity which:

a. is child sexual exploitation and abuse (CSEA);

b. promotes, incites or instructs in matters of violence;

c. is cyber-bullying; and

d. falls under Minecraft's End-User Licence Agreement (EULA) provisions on hate or extreme bias, read together with the "Keep your content clean" section of Xbox's Community Standards and s3(a)(vii) of the Microsoft Services Agreement.[1]

The Expectations are contained in the Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth), which commenced on 24 January 2022. The relevant regulatory guidance is available here.

What you are required to report on

See **Schedule A** for full details of the specific expectations that, under the Notice, the Provider is required to report on.

The decision to give the Notice

I have decided to give the Notice under section 56(2) of the Act. In deciding whether to give a non-periodic reporting notice, I am required by section 56(5) of the Act to have regard to the following criteria, against which I have summarised my considerations:

a) The number of occasions during the previous 12 months on which complaints about material provided on the Service were made to the Commissioner under the Act:
   - During the period 20 March 2025 to 20 March 2026, the eSafety Investigations Branch received 2 complaints relating to material available on the Services, including 1 complaint relating to cyberbullying material; and 1 relating to illegal and restricted content.
   - I do not rely on this factor as a reason for giving this Notice.

b) Whether the provider has previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act:
   - The Provider has not previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act. I do not rely on this factor as a reason for giving this Notice.

c) Whether there are deficiencies in the provider's practices, so far as they relate to the capacity of end-users to use the Service in a safe manner:
   - I note reports from expert agency, research and media reports relating to the potential for unlawful and/or harmful material or activity, as well as harms associated with online gaming services, particularly as they relate to children.
   - I consider that these reports indicate a risk that Australians, especially Australian children, may be exposed to unlawful or harmful material or activity on the Service. The Notice would assist me in understanding what steps the Provider is taking to comply with Expectations 6(2), 6(2A), 11 and 12.

[1] Mojang Studios, 'Minecraft End(er) User Licence Agreement', accessed 24 February 2026, URL: EULA | Minecraft; Xbox, 'Xbox Community Standards', accessed 2 March 2026, Xbox Community Standards | Xbox; Microsoft, 'Microsoft Services Agreement', accessed 3 March 2026, Microsoft Services Agreement.

d) Whether there are deficiencies in the service's terms of use, so far as they relate to the capacity of end-users to use the services in a safe manner:
    - I consider the Notice would assist me in understanding the steps the Provider is taking to enforce its terms of service and comply with Expectation 14(1A).

e) Whether the provider has agreed to give the Secretary regular reports relating to the capacity of end users to use the service in a safe manner;
    - There is no ongoing agreement between the Provider and the Secretary of the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts for regular reports for the purpose of section 56(5)(e). As such, I consider the Notice to be of assistance to exercising my statutory functions.

f) Such other matters (if any) as the Commissioner considers relevant.
    - As well as the considerations above:
        - I consider the use of the Service by Australians to be a risk factor as any failure to comply with the relevant Basic Online Safety Expectations puts Australians at risk, including children.
        - I consider that the Service's features such as its chat functions which enable interaction between children and adults, ability to create user-generated content, immersive features and use of in-app currency are high-risk features with the potential to increase the risk of CSEA activity (e.g. grooming and sexual extortion) and violence material and activity (e.g. youth radicalisation) if appropriate safeguards are not put in place by the Provider.
    - I consider that the following information gaps limit eSafety's understanding of the steps the Provider is taking to ensure safe use and proactively minimise harmful content such as CSEA, violence material and cyberbullying on the Service, including:
        - Quality of training data and effectiveness of moderation tools;
        - Information on content moderators;
        - Information sharing with other providers;
        - Measures to address recidivism.

Additionally, giving the Notice supports my statutory functions as set out in section 27 of the Act, including to promote online safety for Australians, to monitor compliance with the Act, and to collect, analyse, interpret and disseminate information relating to online safety for Australians.

Required action

The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Expectations during the period specified in the Notice and give the report to the Commissioner by **17:00 AEST on 11 May 2026.**

Failure to comply with the Notice may result in the Commissioner taking enforcement action.

You should contact eSafety prior to the Notice deadline if any of the following apply, and take the steps indicated:

- You consider that a question does not apply to your service(s). Provide reasons and an explanation of why the question does not apply.
- You consider that you are not capable of answering a question. Identify the question(s) and provide reasons and an explanation of why you are not capable of answering the question(s). eSafety will consider your reasons and explanation and advise on an appropriate course of action.
- You require additional time to comply with the Notice and to provide the required information. You must request an extension of time from eSafety and provide specific reasons why you are

not capable of meeting the deadline specified in the Notice. eSafety will inform you if an extension of time has been granted by the Commissioner.

- You would like to request an alternative means of returning Schedule B to the Notice other than via Qualtrics. Provide reasons and suggest an alternative method of providing the information. eSafety will arrange appropriate alternate means where appropriate.

eSafety will engage with all providers who contact eSafety. We request that you comply with the instructions given by eSafety in response to any of the above requests.

Extension of time to comply

If the Provider requires additional time to comply with the Notice, please email industryBOSE@esafety.gov.au before **17:00 AEST on 27 April 2026.** In your email, please include reasons for your request.

You may seek an extension of time any time before **17:00 AEST on 27 April 2026**. If you submit a request for an extension of time less than 2 weeks prior to **17:00 AEST on 11 May 2026,** you should include reasons as to why an extension was not sought earlier, as well as reasons for the request.

The deadline in the Notice continues to apply unless eSafety confirms that an extension is granted.

Failure to comply

Under section 57 of the Act, the Provider must comply with the requirement under the Notice to the extent that it is capable of doing so.

Failure to comply with the Notice is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate, following the end of the period specified for compliance with the Notice. eSafety also has a range of other enforcement options, as detailed in the regulatory guidance.

False or misleading information or documents

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to eSafety or the eSafety Commissioner.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Review rights

The Provider has a right to seek an internal or external review of the decision to give a notice to it under section 56(2) of the Act.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

More detailed information about the Provider's review rights is available in the information sheet at Schedule D to this correspondence which sets out the Provider's rights with respect to the different review options available to it, as well as other options if you do not agree with the decision to give the Notice to the Provider.

Confidentiality

eSafety intends to publish a summary of the Provider's responses to the Notice, pursuant to section 217 of the Act. Part of the purpose of collecting the information required under the Notice is publication of that information.

The Provider can make submissions about confidentiality and/or the sensitivity of information provided to eSafety. eSafety will carefully consider any objections when deciding what information to publish. Attachment A to this correspondence outlines the criteria that eSafety will have regard to in considering confidentiality submissions.

The Provider must provide the information required by the Notice even if you have concerns about confidentiality and/or sensitivity of certain information and make submissions to eSafety about the publication of confidential and sensitive information.

eSafety will prepare a summary of information for publication. Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, the Provider will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.

Regards,



Julie Inman Grant
eSafety Commissioner

Enclosed: Notice under section 56(2) of the Act

Information Sheet: Review Rights

NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Mojang AB (the **Provider**)

Attention: s 47F Digital Safety Unit, Microsoft

By Email: s 47F @microsoft.com

This non-periodic reporting notice (**Notice**) is given to Mojang AB (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) in respect of the Minecraft service (the **Service**) that it provides in Australia.

The Provider is required to prepare a report about the extent to which it complied with the applicable Basic Online Safety Expectations specified in **Schedule A** for the period 1 October 2025 to 31 March 2026 inclusive (**Report Period**).

The Provider is required to provide the report in the manner and form specified in **Schedule B,** including following the instructions provided, and answering the questions included in **Schedule B.**

The Provider is required to give the report to the Commissioner within 40 days of being given this Notice, being no later than **17:00 AEST on 11 May 2026** (the **Due Date**), or within such longer period as the Commissioner allows if the Commissioner is contacted by the Provider with a request for an extension of time.

The report is to be given to the Commissioner via the Qualtrics report form in Schedule B of the Notice.

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate.

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Date: 1 April 2026

Julie Inman Grant

eSafety Commissioner

Schedule A – specified applicable basic online safety expectations

The Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) (**Determination**) commenced on 24 January 2022 and contains the Basic Online Safety Expectations, some of which Mojang AB (the **Provider**) as the provider of the Minecraft service (the **Service**), is being required to report on under this Notice. The amendments to the Determination made by the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth) came into effect on 31 May 2024.

This Schedule sets out the specified applicable Basic Online Safety Expectations to be reported on by the Provider for the purpose of this Notice:

Expectations:

6 Expectations—provider will take reasonable steps to ensure safe use

Additional expectation

(2) The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful.

Additional expectation

(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

10 Additional expectation—provider will consult and cooperate with other service providers to promote safe use

Additional expectation

(1) The provider of the service will take reasonable steps to:

(a) consult and cooperate with providers of other services; and

(b) ensure consultation and cooperation occurs between all relevant services provided by that provider, in order to promote the ability of end-users to use all of those services in a safe manner.

11 Core expectation—provider will take reasonable steps to minimise provision of certain material

The provider of the service will take reasonable steps to minimise the extent to which the following material is provided on the service:

(a) cyber-bullying material targeted at an Australian child;

(b) cyber-abuse material targeted at an Australian adult;

(c) a non-consensual intimate image of a person;

(d) class 1 material;

(e) material that promotes abhorrent violent conduct;

(f) material that incites abhorrent violent conduct;

(g) material that instructs in abhorrent violent conduct;

(h) material that depicts abhorrent violent conduct.

12 Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

Core expectation

(1) The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

14 Additional expectations—provider will ensure service has terms of use, certain policies etc.

(1A) The provider of the service will take reasonable steps (including proactive steps) to detect breaches of its terms of use and, where applicable, breaches of policies and procedures in relation to the safety of end-users, and standards of conduct for end-users.

(2) The provider of the service will take reasonable steps (including proactive steps) to ensure that any penalties specified for breaches of its terms of use, policies and procedures in relation to the safety of end-users, and standards of conduct for end-users, are enforced against all accounts held or created by the end-user who breached the terms of use and, where applicable, breached the policies and procedures, and standards of conduct, of the service.

Schedule B - link to Qualtrics report form[2]

This report form constitutes Schedule B to the Notice. It specifies the manner and form of the report required by the Notice and requires you to respond to the questions included within, which relate to the Provider's compliance with the applicable Basic Online Safety Expectations. The relevant expectations are stated alongside each question.

Each of the following is a requirement under the Notice:

- Answer each question truthfully and accurately. Other information provided to the eSafety Commissioner ('eSafety') in relation to the Notice, including statements about a provider's capability to respond to the Notice and submissions related to confidentiality or sensitivity of information, must also be truthful and accurate.
- Use this report form for your response. Responding in an alternative way without prior agreement with eSafety may amount to non-compliance with the Notice.
- Provide a response to each question, and its parts unless the report form states otherwise. Leaving a response blank without providing eSafety with a reasonable explanation in advance of the deadline for the Notice (or any valid extension of time) is likely to be considered as non-compliance with the Notice.
- Provide information for the period from 1 October 2026 to 31 March 2026 (**the Report Period**), unless a question requires information on a specific time period within the Report Period. Some questions may require information as at a specified date. The use of this date within the Report Period ensures that eSafety can obtain up to date information on providers' current practices and aims to reduce the burden on providers.

Navigating through the report form:

- The report form includes single and multiple response options as well as text field options.
- All text fields allow for the available window space to be increased by clicking and dragging the right bottom corner of the box and re-sizing as required.
- A Table of Contents is provided at the top left-hand side to allow for easy navigation though the questions. The forward and back buttons will allow for navigation to any question.
- A response to a question may result in subsequent questions no longer requiring a response. All questions to the report form are displayed, regardless of whether a response is required. This is to provide transparency of the full set of questions.
- Some questions are Provider specific and where there is a question for a different Provider, a note is included to note that the question has been skipped.

---

[2] Link to Qualtrics report from – https://esafetydxm.qualtrics.com/jfe/form/SV_9traCr0DRCfIGKW?Q_CHL=gl&Q_DL=EMD_3dsuwk80bOEmzg4_9traCr0DRCfIGKW_CGC_cFgcY5eomX8ge0e&_g_=g

- Responses are automatically saved in draft and can be revisited over the course of multiple sittings.
- Before submitting the responses, you are required to review all questions to ensure responses are provided.
- Once the report form is submitted, no further changes can be made. You may contact eSafety to reopen a submitted response before the Due Date.
- Once responses are submitted there will be a summary page with an option to download a copy of your responses to a PDF document.

Also note the following:

- Include as much information as is necessary to provide a fulsome response to the question. Question 78 is an opportunity for you to provide information as part of your report about any further safety measures the Provider is taking to comply with these specified expectations.
- You can raise concerns about confidentiality and/or the sensitivity of information. eSafety will carefully consider your submissions when deciding what information to publish. **Attachment A** has been provided to you to outline the criteria that eSafety will have regard to in considering confidentiality submissions. However, concerns about the confidentiality and sensitivity of certain information are not adequate reasons to refuse to provide information required by the Notice. eSafety will prepare a summary of information for publication based on the Provider's responses.
- Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, you will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.
- **Definitions of relevant terms are included in Schedule C to the Notice.** If you have any concerns about the relevant terms, please contact us at industryBOSE@safety.gov.au to discuss.
- Further information can also be found in the Basic Online Safety Expectations Regulatory Guidance and on the relevant page on eSafety's website.
- You can contact industryBOSE@safety.gov.au regarding any of the above information, or with any other questions about your response.
- On the final page where the 'submit' button is displayed, the following text will be included:

  This is the final page of Schedule B to the Notice. Please review your responses. Once you click 'submit', your response will be received by eSafety and all information provided is considered the Provider's response to the Notice. Note that you cannot edit your response after you click 'submit'.

Schedule C – Definitions of relevant terms

The Act: *The Online Safety Act 2021* (Cth).

Age assurance: An umbrella term which includes age verification (determining a person's age to a high level of accuracy, such as through the use of identity documents) age estimation (providing an approximate age through analysis of biological or behavioural human features that vary with age, for example through the use of facial or voice analysis), or age inference (using information other than a date of birth which indirectly implies a certain age or age range).

Child sexual exploitation and abuse (CSEA): Material or activity which includes both:

- 'child sexual exploitation' (a broad category that encompasses material and activity that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse)
- 'child sexual abuse' (which involves a sexual assault against a child, is a narrower category and can be considered a sub-set of child sexual exploitation).

CSEA material is a subset of class 1 material, as defined under section 106 of the Act by reference to the National Classification Scheme, and includes images video and text. CSEA material includes user generated content.

CSEA activity refers to other illegal activity, including grooming and sexual extortion of children. CSEA activity can include attempts to migrate children to a third party service for the purpose of grooming or sexually extorting a child.

See also the definitions in the Industry standards for Relevant Electronic Services regarding class 1A and class 1B material: Register of industry codes and industry standards for online safety | eSafety Commissioner

Class 1 material: Material that is, or would likely be, refused classification (**Refused Classification or RC**) by the Classification Board under the National Classification Scheme. It includes material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence, or
- advocates the doing of a terrorist act.

Class 2 material: Material that is, or would likely be, classified R 18+ or X 18+ under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old (such as pornography, and other high impact material).

Cyberbullying material targeted at an Australian child: Has the meaning given at section 6 of the Online Safety Act 2021.

End-user: A natural person who is an end-user of a product or online service.[3]

Grooming: The process of building an emotional connection with a child in order to sexually abuse or exploit them. This increasingly involves children being tricked or coerced into sexual activity on webcams or into sending sexual images through online services. Grooming is a type of CSEA activity.

Hash-matching tools: Digital technology used to create a unique digital signature (known as a 'hash') of an image or video which is then compared against signatures (hashes) of other photos to find copies of the same image or video.

Hash database: A database of material that has been previously confirmed to contain harmful and/or unlawful material. For example, the Global Internet Forum to Counter Terrorism hash-sharing database.

Language analysis tools: Technologies using methods to assign a probability that text or conversations involve certain behaviour, such as grooming a child for sexual abuse. This may involve artificial intelligence programming.

Material: Defined in section 5 of the Act to mean material, whether in the form of text, data, speech, music or other sounds, visual images (moving or otherwise), of any other form or any combination of forms. In the context of CSEA, 'material' typically refers primarily to images or video content.

Notice: A non-periodic notice given to a provider under section 56(2) of the Act on 1 April 2026.

Online hate policies: Policies relating to either Minecraft's EULA provisions on hate or extreme bias, read together with the "Keep your content clean" section of Xbox's Community Standards and/or s3(a)(vii) of the Microsoft Services Agreement.[4]

Recidivism: In the context of this Notice, banned or suspended users re-registering to a service with the same or new details. Multiple fake or imposter accounts may be created by a human user or by an automated bot programmed by a human.

Report period: When providers receive a reporting Notice from the eSafety Commissioner ('eSafety') they are required to prepare a report about the extent to which they complied with the Expectations during a specified period. This period is referred to as the 'report period'. The report period for this set of Notices is 1 October 2025 to 31 March 2026. Information provided reflects this period, unless stated otherwise.

---

[3] 'Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms', 2025, accessed 18 August 2025, URL: https://onlinesafety.org.au/wp-content/uploads/2025/07/CLEAN-Phase-2-OSA-Codes-Head-Terms-1.pdf

[4] Mojang Studios, 'Minecraft End(er) User Licence Agreement', accessed 24 February 2026, URL: EULA | Minecraft; Xbox, 'Xbox Community Standards', accessed 2 March 2026, Xbox Community Standards | Xbox; Microsoft, 'Microsoft Services Agreement', accessed 3 March 2026, Microsoft Services Agreement.

Sexual extortion: A crime involving online blackmail, where victims are tricked into sending intimate images of themselves to someone who then threatens to share the images unless demands are met, usually for payment. eSafety requires information relating to any instance of sexual extortion, not only those including children. Sexual extortion is a type of CSEA activity.

Violence material and activity: Material or activity which promotes, incites or instructs in matters of crime or violence. Violence material is material which would be, or would likely be, defined as class 2 material for the purposes of section 107 of the Act, or class 1 material for the purposes of section 106 of the Act.

Violence material includes pro-terror material, crime and violence material and extreme crime and violence material as define by the Industry Standards for Relevant Electronic Services: Register of industry codes and industry standards for online safety | eSafety Commissioner. For the purposes of this notice, violence activity may include attempts to migrate children to an external platform for the purposes of sharing violence material (e.g. sharing links to a specific forum or community associated with violence material or activity).

Schedule D - Information sheet: Right of Review

Internal review by the eSafety Commissioner (eSafety)

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things:

- affirm the eSafety Commissioner's decision
- vary the eSafety Commissioner's decision; or
- set the eSafety Commissioner's decision aside and replace it with its own decision.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be waived, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

If we have not provided the reasons for this decision, you may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by eSafety under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to eSafety in writing through one of the following options:

Online: using the **Contact Us** form on eSafety's website

Email: FOI@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal or email address for us to reply to and which we can use to communicate with you about your application.

eSafety's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that eSafety has handled this matter, we ask that you contact us using the **Contact Us** form on eSafety's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with eSafety first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Unlawful and/or harmful material and activity

1. Q1. Does Mojang AB consider the following material and activity types to be unlawful and/or harmful?

	Choose all that apply
CSEA material and activity	☐
Violence material and activity	☐
Cyberbullying	☐
Material and activity covered by Mojang AB's online hate policies	☐

Section 1: Age assurance

Expectations 6(2), 6(2A), 11 and 12.

2. Q2. During the report period, did Mojang AB use tools and techniques to assess the age of end-users on Minecraft?

    a. Yes
    b. No

If yes (a) at Q2

3. Q3. Name all the tools and techniques Mojang AB used to assess the age of end-users on Minecraft and whether the tool or technique was an internal proprietary tool or technique, or provided by a third party.

Name of tool or technology	Internal proprietary tool or technique	Third party tool or technique
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o

If yes to third party tool at Q3

4. Q4. For each third-party tool or technique identified at Q3, specify the name of the third-party provider.

Name of tool/technology	Third party tool provider name
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	

5. Q5. For each tool listed at Q3, specify the type of tool or technique from the list below.

Name of tool/technology	Type of technology or technique used (Drop down list will be displayed with options listed below,)
(Tool from Q3 will be auto populated)	- Self declaration - Facial age estimation - ID document verification (government) - ID document verification (non government) - Credit card verification - Age inference model - Age key - Vouching (parental) - Vouching (other user or institution) - Other
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above

If Other (specify) at Q5 – (only tools where other specify were chose will appear)

6. Q5-1. Specify the 'other' type of tool or technique used.

Name of tool	Specify the type of technology used
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	

If using Age inference models at Q5.

7. Q6. For the age inference models listed in Q5, specify all the indicators that Mojang AB used to assess the age of end users on Minecraft. (multiple response)

	Choose all that apply
Operating system indicators	☐
App store indicators	☐
Cross platform indicators	☐
Language analysis	☐
Voice analysis	☐
Image classifiers	☐
Video classifiers	☐
Device identifiers	☐
IP address indicators	☐
Traffic indicators	☐
Financial indictors	☐
Behavioural indicators (list the behavioural indicators)	☐

Other (specify)	☐
Other (specify)	☐
Other (specify)	☐

If yes (a) at Q2

8. Q7. Specify when each of the tools and techniques listed in response to Q3 were used:

	At sign up	Upon accessing certain game features or parts (eg. text chat, store or particular rooms or areas within a game)	During gameplay	To access certain servers;	When an account has been flagged for review by automated tools/human moderators	In response to a user report	When the service is accessed on a particular device (e.g. console, PC, mobile)	To gain access to parental controls	Other
Name of tool from Q3 will be auto populated)	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐

If *Upon accessing certain game features (e.g. text chat, store)* at Q7 was chosen – (Only tools where this option was chosen will appear)

9. Q7-1. Specify the 'certain game features or parts (e.g. text, chat, store or particular rooms or areas within a game)' on Minecraft where the tool or technique was used.

Name of tool	Game features tool was used in
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

If other (specify) was chosen for any response at Q7

10. Q7-2. Specify when the 'other' tool or technique was used on Minecraft.

Name of tool	Specify
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	

If used a tool to assess the age of end-users (Yes at Q2)

11. Q8. During the report period, did Mojang AB or a third-party provider of a tool or technique assess the effectiveness of these tools and techniques used on Minecraft?

Name of tool/technology	Yes – Mojang AB assessed	Yes – Third-party provider assessed	No
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o
(Tool from Q3 will be auto populated)	☐	☐	o

If yes at Q8 (assessed accuracy of the tools)

12. Q9. What metrics did Mojang AB (or the third-party provider of a tool or technique) use to assess the effectiveness of each tool and technique? Include the specific metrics, and any relevant standards or certification schemes that Mojang AB relied on to evaluate the effectiveness of a tool in your answer.

Name of tool/technology	Specify the effectiveness metric used for the assessment
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

13. Q10. What was the result of the assessment for effectiveness of each tool and technique?

Name of tool/technology	Specify details of the result
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

14. Q11. What action was taken as a result of the assessment for each tool and technique?

Name of tool/technology	Specify the action taken
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

15. Q12. During the report period, what action did Mojang AB take after it became aware that the age information it held about an end-user may be incorrect.

	Choose all that apply
Banned account	☐
Suspended account	☐
Directed to undergo age assurance	☐
Strike against account	☐
Other (specify)	☐

IF yes at Q2

16. Q13. During the report period, specify how many end-users were found to be incorrectly age assured by the tools and techniques identified at Q3 to assess the age of end-users.

16. Q14. Provide any other relevant information or context in relation to your responses to questions 1 to 13, including:
    a. whether Mojang AB undertook any research or development work during the report period in relation to age assurance
    b. whether responses to these questions are affected by whether an end-user is using Bedrock edition or Java edition, or is using Minecraft Realms, Featured Bedrock Servers, user hosted experiences or third party unaffiliated servers
    c. whether responses to these questions are affected by whether an end-user uses Minecraft on particular devices (e.g. on a particular console, PC, or mobile)

Section 2: Staffing / Moderation

Expectations 6(2), 6(2A), 11 and 12.

17. Q15. As at 31 March 2026, provide the number of staff employed by Mojang AB for the below categories.

	Specify number employed
Engineers employed by Mojang AB who spend at least 50% of their time on trust and safety	
Content moderators employed by Mojang AB	
Content moderators contracted employed by Mojang AB	
Trust and safety staff employed by Mojang AB (other than engineers and content moderators)	

18. Q16. As at 31 March 2026, provide the number of moderators (contracted or employed by Mojang AB) trained in the following unlawful or harmful material or activity:

	Specify number of moderators trained in each following unlawful or harmful material or activity
Grooming	
Other CSEA material and activity	
Sexual extortion	
Violence material and activity	

19. Q17. As at 31 March 2026, specify which of the below languages Mojang AB's trust and safety staff operated in.

	Choose all that apply
English	☐
Mandarin	☐
Arabic	☐
Vietnamese	☐
Cantonese	☐
Punjabi	☐
Other languages	☐

If other (specify) was chosen for any response at Q17

20. Q18. What is the total number of the **other** languages that the Mojang AB's contractor trust and safety staff operated in?

Number of other languages (excluding those listed at Q17)	

21. Q19. Provide any other relevant information or context in relation to your responses to questions 15 to Q18.

Section 3: User reporting

Expectations 14(1A).

22. Q20 During the report period, specify the number of **global** end-user reports of unlawful or harmful material or activity on Minecraft which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

    Include reports from all Minecraft servers, including third party unaffiliated servers.

	Number of **global** end-user reports
Grooming	
Sexual extortion	
Other CSEA material) and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Mojang AB's online hate policies	

23. Q21. During the report period, specify the number of **Australian** end-user reports of unlawful or harmful material or activity on Minecraft which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Number of **Australian** end-user reports
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Mojang AB's online hate policies	

24. Q22. During the report period, specify the median time taken to reach an outcome after an end-user made a report, where reports were reviewed by human moderators. Provide responses for the median time concerning each of the following unlawful or harmful material or activity on Minecraft.

This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review.

Provide a response in minutes

	Median time taken (minutes)
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	

Material and activity covered by Mojang AB's online hate policies	

25. Q23. During the report period, specify the median time taken to reach an outcome after automated tools flagged potential unlawful or harmful material or activity on Minecraft, where flags were reviewed by human moderators. Specify for each of the following unlawful or harmful material or activity.

    This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review

	Median time taken
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Mojang AB's online hate policies	

26. Q24. During the report period, specify the proportion in percentage of unlawful or harmful material or activity that was detected proactively vs reported by users on Minecraft, concerning the following unlawful or harmful material or activity.

	Detected proactively (%)	Reported by end-users (%)
Grooming		
Sexual extortion		
Other CSEA material and activity		
Violence material and activity		
Cyber-bullying		
Material and activity covered by Mojang AB's online hate policies		

27. Q25. Explain how the answers to questions Q20 to Q24 were calculated and provide any other context.

	Specify how answers were calculated and provide any other context
Number of **Global** end-user reports	
Number of **Australian** end-user reports	
Median time taken to reach outcome from **Global** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from **Australian** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from automated tools that were reviewed by human moderators	
Percentage of unlawful or harmful material or activity detected proactively vs reported by users	

Section 4: Action taken against end-users

Expectations 14(1A) and 14(2)

28. Q26. During the report period, what action did Mojang AB take after an end-user breached the terms of service and/or community guidelines (or equivalent) in relation to the following unlawful or harmful material or activity.

	Sexual extortion	Grooming	Other CSEA material and activity	Violence material and activity	Cyberbullying	Conduct that breaches Mojang AB's online hate policies
Banned account	☐	☐	☐	☐	☐	☐
Suspended account	☐	☐	☐	☐	☐	☐
Strike/Warning given to end-user	☐	☐	☐	☐	☐	☐
Restricted player's access to certain features of the game (e.g. ability to interact with other players)	☐	☐	☐	☐	☐	☐
Removed harmful content created by user (e.g. user-generated content, messages)	☐	☐	☐	☐	☐	☐
Prevented user from creating certain content (e.g. marketplace items)	☐	☐	☐	☐	☐	☐
Other (specify)	☐		☐ ☐	☐	☐	☐

29. Q27. During the report period, were Mojang AB's trust and safety staff automatically informed when operators of third party unaffiliated servers or Bedrock Featured servers banned an account from their server for behaviour related to the following unlawful or harmful material or activity.

	Yes	No
Grooming	○	○
Sexual extortion	○	○
Other CSEA material and activity	○	○
Violence material and activity	○	○

Material and activity covered by Mojang AB's online hate policies	○	○

If trust and safety were not informed automatically at Q27 – No to at least 1.

30. Q28. How did Mojang AB ensure that a user banned from an Third-Party Unaffiliated server or Bedrock Featured server for breaches related to the unlawful or harmful material or activity at Q27 was not able to engage in this activity on other parts of the service?

31. Q29. Provide any other relevant information or context in relation to your responses to questions 26 to 28, including whether responses to these questions are affected by whether an end-user is using Bedrock edition or Java edition, is using Minecraft Realms, Featured Bedrock Servers, user hosted experiences or third party unaffiliated servers, or is using Minecraft on particular devices (e.g. on a particular console, PC, or mobile)

Section 5: Tools and Techniques

Expectations 6(2), 6(2A), 11 and 12.

32. Q30. During the report period, did Mojang AB use tools and/or techniques on Minecraft to detect the following unlawful or harmful material or activity?

	Yes	No
Grooming	○	○
Sexual extortion	○	○
Other CSEA material and activity	○	○
Violence material and activity	○	○
Attempts to migrate children to another service	○	○

If used tool/techniques to identify harms (Yes for any at Q30)

33. Q31. Name all the tools and techniques used and which harm types they cover.

	Grooming [IF yes to Grooming at Q29]	Sexual extortion [IF yes to Sexual extortion at Q29]	Other CSEA material and activity [IF yes to Other CSEA at Q29]	Violence material and activity [IF yes to Violence at Q29]	Attempts to migrate children to another service [IF yes to attempts to migrate at Q29]
Tool 1 (Specify)	☐	☐	☐	☐	☐
Tool 2 (Specify)	☐	☐	☐	☐	☐

Tool 3 (Specify)	☐	☐	☐	☐	☐
Tool 4 (Specify)	☐	☐	☐	☐	☐
Tool 5 (Specify)	☐	☐	☐	☐	☐
Tool 6 (Specify)	☐	☐	☐	☐	☐
Tool 7 (Specify)	☐	☐	☐	☐	☐
Tool 8 (Specify)	☐	☐	☐	☐	☐
Tool 9 (Specify)	☐	☐	☐	☐	☐
Tool 10 (Specify)	☐	☐	☐	☐	☐

If used tool/techniques to identify violence material or violence activity at Q31

34. Q32. Specify the types of 'violence material and/or activity' the tool/technique is used to identify.

	Specify below
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	

If used tool/techniques to identify harms (Yes for any at Q30)

35. Q33. For each tool and technique identified at Q31, specify which part of the service it is used on.

[Minecraft response options]	Featured Bedrock servers	Third party unaffiliated servers	Minecraft Realms servers	User-hosted servers	Interactions between avatars	Creation of certain shapes (e.g. a swastika, making words out of blocks)	Text chat	Text on books	Minecraft store items (e.g. skins)	Other (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

IF other at Q33

36. Q33-1. Specify the 'other' part of the service where the tool or technique was used.

	Specify
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	

If Minecraft + no third-party unaffiliated servers selected in Q33

36. Q33-2. If Mojang AB did not use proactive moderation on third party unaffiliated servers during the report period, explain why this was not possible or practicable.

If used tool/techniques to identify harms (Yes for any at Q30)

37. Q34. For each tool and technique identified at Q31, specify the type of tool or technique.

	Language analysis tool (text) `	Language analysis tool (audio)	AI classifier	Hash-matching tool	Signals-based detection (e.g. behavioural indicators, financial indicators (specify)	Other (e.g. detecting URL join links) (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐

If Other (specify) chosen for any tool at Q34.

37. Q34-1. Specify the other type of tool or technique for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

If Signals-based detection (specify) chosen for any tool at Q34.

38. Q35. Specify the signals used for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

39. Q36. For each tool or technique identified Q31, specify whether the tool detects material before or after it is published (i.e. as part of a pre-screening process).

	Before material is published	After material is published	Provide any relevant details
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	

If used hash-matching tool at Q34

40. Q37. For each hash-matching tool identified at Q34, specify the names of the hash-matching source databases used.

Choose all that apply.

	GIFCT	IWF	NCMEC	Other (specify)
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	

Q37-1. Please specify the 'other' hash-matching source database for the tools below.

	Other (specify)
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

41. Q38. For each hash-matching tool identified at Q34, specify the frequency at which Mojang AB updated the hashes it scanned on Minecraft against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (Specify)
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will	○	○	○	○	○	○

auto populate)						
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○

41. Q38-1. Specify the 'other' frequency at which Mojang AB updated the hashes it scanned on Minecraft against these databases.

	Specify
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

IF used language analysis tool at Q34

42. Q39. For each language analysis tool identified at Q34, specify all the languages it operated in.

Choose all that apply.

	English	Mandarin	Arabic	Vietnamese	Cantonese	Punjabi	Other	Language agnostic
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐

If other (specify) was chosen for any response at Q39

43. Q40. What is the total number of **other** languages that the language analysis tool operated in?

Number of other languages (excluding those listed at Q39)	

If use language analysis tool at Q34

44. Q41. For each language analysis tool identified at Q34, specify whether the tool has been trained to do any of the following:

	Key-word detection	Interpret sentence level context	Interpret conversation-level context	Distinguish joking/irony from serious intent	Interpret coded or indirect language (including use of emojis or symbols in words)	Interpret formatting or hashtags as context clues	Detect coercive or manipulative language	Detect attempts to migrate children to another service	Provide any other relevant details
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	

If tool used language analysis tools at Q34

45. Q42. List all the organisations used to source keywords/training data for the language analysis tools listed below.

	GIFCT	IWF	NCMEC	Lantern	Other (specify)
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	

IF other at Q42

45. Q42-1. Provide details on the other organisations used to source keyword/training data for the language analysis tools.

	Other (specify)
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	

If tool used language analysis tools at Q34

46. Q43. For each language analysis tool identified at Q34, specify the frequency Mojang AB updated the tool against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (specify)
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○

(Language analysis tool from Q34 will auto populate)	o	o	o	o	o	o
(Language analysis tool from Q34 will auto populate)	o	o	o	o	o	o

IF other at Q43

46. Q43-1. Provide details on the frequency that Mojang AB updated the language analysis tools against the source keyword/training data.

47. ASK ALL who use tools Q33 yes Q44. During the report period, did Mojang AB assess the accuracy of all the below tools used to detect the unlawful or harmful material or activity?

	Yes	No
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o

If assessed accuracy of tools (Yes at Q44)

48. Q45. Provide details of the assessment methodology, specify details of any red teaming or simulated adversarial testing.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

49. Q46. What were the results of this assessment? Include **precision** and **recall rates** in your answer, and/or **any other metrics used to quantify the result**, with relevant context.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

50. Q47. What action was taken as a result of the assessment for each tool?

	Specify action taken
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

51. Q48. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **Grooming**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Grooming at Q48.

57. Q48-1. If only in certain circumstances for Grooming, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	

53. Q49. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **sexual extortion**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for sexual extortion at Q49

57. Q49-1. If only in certain circumstances for sexual extortion, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	

54. Q50. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **other CSEA material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Other CSEA at Q50

57. Q50-1. If only in certain circumstances for other CSEA material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	

(Tool from Q50 that are used in some circumstances will auto populate)	

55. Q51. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **violence material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for violence material and activity at Q51

57. Q51-1. If only in certain circumstances for violence material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	

56. Q52. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances **on attempts to migrate children to another service**?

	Used on all material by default	Used on material in some circumstance
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for attempts to migrate children at Q52

57. Q52-1. If only in certain circumstances on attempts to migrate children to another service, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances

(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	

58. Q53. During the report period, did Mojang AB take steps to identify servers, including third party unaffiliated servers which may be higher risk for grooming, sexual extortion, other CSEA material and activity, violence material and activity and/or material and activity captured by [Provider's] online hate policies? Y/N

If Yes at Q53

59. Q54. Specify any measures used by Mojang AB, in addition to the tools and techniques identified at Q31 to address grooming, sexual extortion, other CSEA material and activity, violence material and activity and online hate policies on these higher risk servers.

60. Q55. During the report period, did Mojang AB use any tools or other measures to detect transactions of Minecoins and/or Minecoin gift cards that may be linked to grooming and/or sexual extortion?

    1. Yes (specify details)
    2. No

61. Q56. Specify the details of the tools or other measures used to detect transactions of Minecoins or Minecoin gift cards that may be linked to grooming and/or sexual extortion.

62. Q57. Provide any other relevant information or context in relation to your responses to questions 39 to 46, including:
    a. whether Mojang AB undertook any research or development work during the report period in relation to proactive detection of the harms listed in Q30
    b. whether responses to these questions are affected by whether an end-user is using Bedrock edition or Java edition, or is using Minecraft Realms, Featured Bedrock Servers, user hosted experiences or third party unaffiliated servers
    c. whether responses to these questions are affected by whether an end-user uses Minecraft on particular devices (e.g. on a particular console, PC, or mobile)

Section 6: Recidivism

Expectations 14(1A).

63. Q58. During the report period, did Mojang AB use the below indicators to identify recidivism after an end user had been banned or suspended for CSEA or violence material and activity.

	CSEA	Sexual extortion	Violence material and activity
Device identifiers	☐	☐	☐
Phone number	☐	☐	☐
Behavioural indicators	☐	☐	☐
Email address	☐	☐	☐
Geographical indicators	☐	☐	☐
Financial indicators	☐	☐	☐
Profile picture	☐	☐	☐
Username	☐	☐	☐
Name	☐	☐	☐
Date of birth	☐	☐	☐
Display name	☐	☐	☐
Other (specify)	☐	☐	☐
Other (specify)	☐	☐	☐

If used indicators to identify recidivism at Q58.

64. Q59. Were indicators used by default in all cases where an account has been banned or suspended for **CSEA material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

65. Q60. Were indicators used by default in all cases where an account has been banned or suspended for **sexual extortion**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

66. Q61. Were indicators used by default in all cases where an account has been banned or suspended for **violence material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

If used indicators to identify recidivism at Q58.

67. Q62. What specific action did Mojang AB take based on these indicators? If the action taken differed based on the specific indicators, specify all those differences, e.g. automatically blocked accounts with these indicators from being created; flagged the account for human review etc.

	Specify action taken
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	

68. Q63. Provide any other relevant information or context in relation to your responses to questions 58 to 62 including:
    a. whether Mojang AB undertook any research or development work during the report period in relation to prevention of recidivism on Minecraft
    b. whether responses to these questions are affected by whether an end-user is using Bedrock edition or Java edition, or is using Minecraft Realms, Featured Bedrock Servers, user hosted experiences or third party unaffiliated servers
    c. whether responses to these questions are affected by whether an end-user uses Minecraft on particular devices (e.g. on a particular console, PC, or mobile)

Section 7: Moderation of user-generated content

69. Q64. During the report period, did Mojang AB share information with or otherwise collaborate with third parties to prevent creation of mods or servers that violate Minecraft's Usage Guidelines?
    a. Yes
    b. No

IF yes at Q48c.

70. Q65. Specify how Mojang AB collaborated or shared information with third party providers, including operators of servers on the Bedrock Featured Servers List and the Official Minecraft Server List, in order to prevent the creation of mods or servers that violate Minecraft's Usage Guidelines.

70. Q65-1. Specify any other measures that Mojang AB took to prevent the creation of third-party mods that allowed materials in breach of its Usage Guidelines.

Section 8: Information sharing initiatives

Expectations 10(1) and 14(1A).

71. Q66. During the report period, did Mojang AB share information with the following services or initiatives (including bi-lateral arrangements with other providers) for the purpose of minimising grooming/sexual extortion and violence material and activity on its service?

	Choose all that apply
Lantern	☐
Tech Coalition	☐
Fair Play Alliance	☐
Tech Against Terrorism	☐
Discord	☐
Twitch	☐
Steam	☐
Other Initiatives/Services (specify)	☐

If a member of information sharing initiative (any at Q66)

72. Q67. Explain the steps taken as a result of sharing information with the below initiatives.

	Specify steps taken
(Auto populate sharing initiative chosen at Q669)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	

73. Q68. Provide any other relevant information or context in relation to your responses to questions 66 to 67, including whether Mojang AB undertook any research or development work during the report period in relation to collaborating with civil society organisations or other service providers to prevent harm on Minecraft

Section 9: Off-platform monitoring

Expectations 6(2), 6(2A), 11 and 12.

74. Q69. During the report period, did Mojang AB use off-platform monitoring (monitoring of activity on other services either provided internally or by third-party services) to identify accounts or communities present on its service that are engaged in the below harms.

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Violence activity	o	o

If used off-platform monitoring (Yes at Q69)

74. Q70. Provide details, specifying what this involved and what third party services were used.

	Specify details	Specify names of third parties used
Grooming		
Sexual extortion		
Violence activity		

75. Q71. Provide any other relevant information or context in relation to your responses to Q69 and Q70 , including whether Mojang AB undertook any research or development work during the report period in relation to monitoring of other services to identify accounts or communities engaged in the harms listed at Q69.

Section 10: Other

Expectations 6(2), 6(2A) and 11.

76. Q72. During the report period, did Mojang AB provide any help services or support to users who were identified as potential victims of grooming and/or sexual extortion?
    a. Yes
    b. No

IF yes at Q53

77. Q73. Provide details on the help services or support Mojang AB provided to users who were identified as potential victims of grooming and/or sexual extortion.

78. Q74. As at 31 March 2026, specify the proportion of under 18 accounts in Australia that have parental supervision enabled.

79. Q75. Explain how the answer to Q74 was calculated and provide any other context, including whether the use of parental controls on Minecraft are affected by whether an end-user uses Minecraft on particular devices (e.g. on a particular console, PC, or mobile).

Section 11: Final question

80. Q78. Outline any further steps Mojang AB is taking to meet Expectations 6(2), 6(2A), 10(1), 11, 12, 14(1A) and 14(2).

    Do not replicate information provided in previous responses here. This is an opportunity for Mojang AB to outline information about other types of safety measures.

1 April 2026

Our reference: BOSE-2026-103

Roblox Corporation

c/o s 47F

By email: s 47F @roblox.com, cc s 47F @roblox.com

Dear s 47F ,

Non-periodic reporting notice requiring Roblox Corporation to prepare a report about the extent to which it has complied with the Basic Online Safety Expectations

The eSafety Commissioner is responsible for improving and promoting online safety for Australians. This includes giving notices to service providers about their compliance with the Basic Online Safety Expectations (**the Expectations**), and publishing summaries of our findings. For more information about eSafety's role and functions, please refer to our website.

The publication of findings serves to increase the transparency and accountability of online services in demonstrating the actions that they are taking to protect Australians from harms online. Transparency also empowers Australians with information to better understand the online environment and any safety risks that may be present on services.

By highlighting what we have learned from notices, eSafety's aim is that the information is also used by researchers, academics, the media and the public to scrutinise the efforts of industry to encourage implementation of the Expectations and to lift safety practices, protections and standards across the industry.

Please see enclosed a non-periodic reporting notice (**the Notice**) given to Roblox Corporation (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**). The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Basic Online Safety Expectations during the period specified in the Notice in respect to the Roblox service (**the Service**).

The Notice requires the Provider to give the report to the Commissioner by **17:00 Australian Eastern Standard Time (AEST) on 11 May 2026.**

If you require additional time to comply with the Notice, you may request this by sending an email to industryBOSE@esafety.gov.au before **17:00 AEST on 27 April 2026.**

The manner and form of the required report are included in **Schedule B** to the Notice. Instructions on this requirement are included in the Notice. Definitions of relevant terms are included in **Schedule C** to the Notice.

The specified applicable Basic Online Safety Expectations

The Notice focuses on the steps being taken to comply with the Expectations, with a focus on the following unlawful and/or harmful material and activity:

a. is child sexual exploitation and abuse (CSEA);

b. promotes, incites or instructs in matters of violence;

c. is cyber-bullying; and

d. falls under the Provider's community standards on 'Discrimination, Slurs and Hate Speech'.[1]

The Expectations are contained in the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth), which commenced on 24 January 2022. The relevant regulatory guidance is available here.

What you are required to report on

See **Schedule A** for full details of the specific expectations that, under the Notice, the Provider is required to report on.

The decision to give the Notice

I have decided to give the Notice under section 56(2) of the Act. In deciding whether to give a non-periodic reporting notice, I am required by section 56(5) of the Act to have regard to the following criteria, against which I have summarised my considerations:

a) The number of occasions during the previous 12 months on which complaints about material provided on the Service were made to the Commissioner under the Act:
   - During the period 20 March 2025 to 20 March 2026, the eSafety Investigations Branch received 163 complaints relating to material available on the Services, including 62 complaints relating to cyberbullying material; 7 relating to Imaged based abuse; and 64 relating to illegal and restricted content.
   - I do not rely on this factor as a reason for giving this Notice.

b) Whether the provider has previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act:
   - The Provider has not previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act. I do not rely on this factor as a reason for giving this Notice.

c) Whether there are deficiencies in the provider's practices, so far as they relate to the capacity of end-users to use the services in a safe manner:
   - I note reports from expert agency, research and media reports relating to the potential for unlawful and/or harmful material or activity, as well as harms associated with online gaming services, particularly as they relate to children.
   - I consider that these reports indicate a risk that Australians, especially Australian children, may be exposed to unlawful or harmful material or activity on the Service. The

[1] Roblox, 'Roblox Community Standards', accessed 25 February 2026, URL: Roblox Community Standards | Roblox.

Notice would assist me in understanding what steps the Provider is taking to comply with Expectations 6(2), 6(2A), 11 and 12.

d) Whether there are deficiencies in the service's terms of use, so far as they relate to the capacity of end-users to use the services in a safe manner:
    - I consider the Notice would assist me in understanding the steps the Provider is taking to enforce its terms of service and comply with Expectation 14(1A).
e) Whether the provider has agreed to give the Secretary regular reports relating to the capacity of end users to use the service in a safe manner;
    - There is no ongoing agreement between the Provider and the Secretary of the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts for regular reports for the purpose of section 56(5)(e). As such, I consider the Notice to be of assistance to exercising my statutory functions.
f) Such other matters (if any) as the Commissioner considers relevant.
    - As well as the considerations above:
        - I consider the use of the Service by Australians to be a risk factor as any failure to comply with the relevant Basic Online Safety Expectations puts Australians at risk, including children.
        - s 47G(1)(a) [redacted]
    - I consider that the following, but not limited to, information gaps limit eSafety's understanding of the steps the Provider is taking to ensure safe use and proactively minimise harmful content such as CSEA, violence material and cyberbullying on the Service:
        - Quality of training data and effectiveness of moderation tools;
        - Information on content moderators;
        - Information sharing with other providers;
        - Measures to address recidivism.

Additionally, giving the Notice supports my statutory functions as set out in section 27 of the Act, including to promote online safety for Australians, to monitor compliance with the Act, and to collect, analyse, interpret and disseminate information relating to online safety for Australians.

Required action

The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Expectations during the period specified in the Notice and give the report to the Commissioner by **17:00 AEST on 11 May 2026.**

Failure to comply with the Notice may result in the Commissioner taking enforcement action.

You should contact eSafety prior to the Notice deadline if any of the following apply, and take the steps indicated:

- You consider that a question does not apply to your service(s). Provide reasons and an explanation of why the question does not apply.
- You consider that you are not capable of answering a question. Identify the question(s) and provide reasons and an explanation of why you are not capable of answering the question(s).

eSafety will consider your reasons and explanation and advise on an appropriate course of action.

- You require additional time to comply with the Notice and to provide the required information. You must request an extension of time from eSafety and provide specific reasons why you are not capable of meeting the deadline specified in the Notice. eSafety will inform you if an extension of time has been granted by the Commissioner.
- You would like to request an alternative means of returning Schedule B to the Notice other than via Qualtrics. Provide reasons and suggest an alternative method of providing the information. eSafety will arrange appropriate alternate means where appropriate.

eSafety will engage with all providers who contact eSafety. We request that you comply with the instructions given by eSafety in response to any of the above requests.

Extension of time to comply

If the Provider requires additional time to comply with the Notice, please email industryBOSE@esafety.gov.au before **17:00 AEST on 27 April 2026.** In your email, please include reasons for your request.

You may seek an extension of time any time before **17:00 AEST on 27 April 2026**. If you submit a request for an extension of time less than 2 weeks prior to **17:00 AEST on 11 May 2026**, you should include reasons as to why an extension was not sought earlier, as well as reasons for the request.

The deadline in the Notice continues to apply unless eSafety confirms that an extension is granted.

Failure to comply

Under section 57 of the Act, the Provider must comply with the requirement under the Notice to the extent that it is capable of doing so.

Failure to comply with the Notice is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate, following the end of the period specified for compliance with the Notice. eSafety also has a range of other enforcement options, as detailed in the regulatory guidance.

False or misleading information or documents

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to eSafety or the eSafety Commissioner.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Review rights

The Provider has a right to seek an internal or external review of the decision to give a notice to it under section 56(2) of the Act.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

More detailed information about the Provider's review rights is available in the information sheet at Schedule D to this correspondence which sets out the Provider's rights with respect to the different review options available to it, as well as other options if you do not agree with the decision to give the Notice to the Provider.

Confidentiality

eSafety intends to publish a summary of the Provider's responses to the Notice, pursuant to section 217 of the Act. Part of the purpose of collecting the information required under the Notice is publication of that information.

The Provider can make submissions about confidentiality and/or the sensitivity of information provided to eSafety. eSafety will carefully consider any objections when deciding what information to publish. Attachment A to this correspondence outlines the criteria that eSafety will have regard to in considering confidentiality submissions.

The Provider must provide the information required by the Notice even if you have concerns about confidentiality and/or sensitivity of certain information and make submissions to eSafety about the publication of confidential and sensitive information.

eSafety will prepare a summary of information for publication. Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, the Provider will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.

Regards,



Julie Inman Grant
eSafety Commissioner

Enclosed: Notice under section 56(2) of the Act

Information Sheet: Review Rights

NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Roblox Corporation (the **Provider**)

Attention: s 47F Roblox Corporation

By Email: s 47F @roblox.com

This non-periodic reporting notice (**Notice**) is given to Roblox Corporation (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) in respect of the Roblox service (the **Service**) that it provides in Australia.

The Provider is required to prepare a report about the extent to which it complied with the applicable Basic Online Safety Expectations specified in **Schedule A** for the period 1 October 2025 to 31 March 2026 inclusive (**Report Period**).

The Provider is required to provide the report in the manner and form specified in **Schedule B,** including following the instructions provided, and answering the questions included in **Schedule B.**

The Provider is required to give the report to the Commissioner within 40 days of being given this Notice, being no later than **17:00 AEST 11 May 2026** (the **Due Date**), or within such longer period as the Commissioner allows if the Commissioner is contacted by the Provider with a request for an extension of time.

The report is to be given to the Commissioner via the Qualtrics report form in Schedule B of the Notice.

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate.

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Date: 1 April 2026



Julie Inman Grant

eSafety Commissioner

Schedule A – specified applicable basic online safety expectations

The Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) (**Determination**) commenced on 24 January 2022 and contains the Basic Online Safety Expectations, some of which Roblox Corporation (the **Provider**) as the provider of the Roblox service (the **Service**), is being required to report on under this Notice. The amendments to the Determination made by the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth) came into effect on 31 May 2024.

This Schedule sets out the specified applicable Basic Online Safety Expectations to be reported on by the Provider for the purpose of this Notice:

Expectations:

6 Expectations—provider will take reasonable steps to ensure safe use

Additional expectation

(2) The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful.

Additional expectation

(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

10 Additional expectation—provider will consult and cooperate with other service providers to promote safe use

Additional expectation

(1) The provider of the service will take reasonable steps to:

(a) consult and cooperate with providers of other services; and

(b) ensure consultation and cooperation occurs between all relevant services provided by that provider, in order to promote the ability of end-users to use all of those services in a safe manner.

11 Core expectation—provider will take reasonable steps to minimise provision of certain material

The provider of the service will take reasonable steps to minimise the extent to which the following material is provided on the service:

(a) cyber-bullying material targeted at an Australian child;

(b) cyber-abuse material targeted at an Australian adult;

(c) a non-consensual intimate image of a person;

(d) class 1 material;

(e) material that promotes abhorrent violent conduct;

(f) material that incites abhorrent violent conduct;

(g) material that instructs in abhorrent violent conduct;

(h) material that depicts abhorrent violent conduct.

12 Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

Core expectation

(1) The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

Examples of reasonable steps that could be taken

14 Additional expectations—provider will ensure service has terms of use, certain policies etc.

(1A) The provider of the service will take reasonable steps (including proactive steps) to detect breaches of its terms of use and, where applicable, breaches of policies and procedures in relation to the safety of end-users, and standards of conduct for end-users.

(2) The provider of the service will take reasonable steps (including proactive steps) to ensure that any penalties specified for breaches of its terms of use, policies and procedures in relation to the safety of end-users, and standards of conduct for end-users, are enforced against all accounts held or created by the end-user who breached the terms of use and, where applicable, breached the policies and procedures, and standards of conduct, of the service.

Schedule B - link to Qualtrics report form[2]

This report form constitutes Schedule B to the Notice. It specifies the manner and form of the report required by the Notice and requires you to respond to the questions included within, which relate to the Provider's compliance with the applicable Basic Online Safety Expectations. The relevant expectations are stated alongside each question.

Each of the following is a requirement under the Notice:

- Answer each question truthfully and accurately. Other information provided to the eSafety Commissioner ('eSafety') in relation to the Notice, including statements about a provider's capability to respond to the Notice and submissions related to confidentiality or sensitivity of information, must also be truthful and accurate.
- Use this report form for your response. Responding in an alternative way without prior agreement with eSafety may amount to non-compliance with the Notice.
- Provide a response to each question, and its parts unless the report form states otherwise. Leaving a response blank without providing eSafety with a reasonable explanation in advance of the deadline for the Notice (or any valid extension of time) is likely to be considered as non-compliance with the Notice.
- Provide information for the period from 1 October 2025 to 3 March 2026 (**the Report Period**), unless a question requires information on a specific time period within the Report Period. Some questions may require information as at a specified date. The use of this date within the Report Period ensures that eSafety can obtain up to date information on providers' current practices and aims to reduce the burden on providers.

Navigating through the report form:

- The report form includes single and multiple response options as well as text field options.
- All text fields allow for the available window space to be increased by clicking and dragging the right bottom corner of the box and re-sizing as required.
- A Table of Contents is provided at the top left-hand side to allow for easy navigation though the questions. The forward and back buttons will allow for navigation to any question.
- A response to a question may result in subsequent questions no longer requiring a response. All questions to the report form are displayed, regardless of whether a response is required. This is to provide transparency of the full set of questions.
- Some questions are Provider specific and where there is a question for a different Provider, a note is included to note that the question has been skipped.

---

[2] Link to Qualtrics report form – https://esafetydxm.qualtrics.com/jfe/form/SV_9traCr0DRCfIGKW?Q_CHL=gl&Q_DL=EMD_3dsuwk80bOEmzg4_9traCr0DRCfIGKW_CGC_mo6r3YDyOc9Mcai&_g_=g

- Responses are automatically saved in draft and can be revisited over the course of multiple sittings.
- Before submitting the responses, you are required to review all questions to ensure responses are provided.
- Once the report form is submitted, no further changes can be made. You may contact eSafety to reopen a submitted response before the Due Date.
- Once responses are submitted there will be a summary page with an option to download a copy of your responses to a PDF document.

Also note the following:

- Include as much information as is necessary to provide a fulsome response to the question. Question 78 is an opportunity for you to provide information as part of your report about any further safety measures the Provider is taking to comply with these specified expectations.
- You can raise concerns about confidentiality and/or the sensitivity of information. eSafety will carefully consider your submissions when deciding what information to publish. Attachment A has been provided to you to outline the criteria that eSafety will have regard to in considering confidentiality submissions. However, concerns about the confidentiality and sensitivity of certain information are not adequate reasons to refuse to provide information required by the Notice. eSafety will prepare a summary of information for publication based on the Provider's responses.
- Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, you will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.
- **Definitions of relevant terms are included in Schedule C to the Notice.** If you have any concerns about the relevant terms, please contact us at industryBOSE@safety.gov.au to discuss.
- Further information can also be found in the Basic Online Safety Expectations Regulatory Guidance and on the relevant page on eSafety's website.
- You can contact industryBOSE@safety.gov.au regarding any of the above information, or with any other questions about your response.
- On the final page where the 'submit' button is displayed, the following text will be included:

  This is the final page of Schedule B to the Notice. Please review your responses. Once you click 'submit', your response will be received by eSafety and all information provided is considered the Provider's response to the Notice. Note that you cannot edit your response after you click 'submit'.

Schedule C – Definitions of relevant terms

The Act: *The Online Safety Act 2021* (Cth).

Age assurance: An umbrella term which includes age verification (determining a person's age to a high level of accuracy, such as through the use of identity documents) age estimation (providing an approximate age through analysis of biological or behavioural human features that vary with age, for example through the use of facial or voice analysis), or age inference (using information other than a date of birth which indirectly implies a certain age or age range).

Child sexual exploitation and abuse (CSEA): Material or activity which includes both:

- 'child sexual exploitation' (a broad category that encompasses material and activity that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse)
- 'child sexual abuse' (which involves a sexual assault against a child, is a narrower category and can be considered a sub-set of child sexual exploitation).

CSEA material is a subset of class 1 material, as defined under section 106 of the Act by reference to the National Classification Scheme, and includes images video and text. CSEA material includes user generated content.

CSEA activity refers to other illegal activity, including grooming and sexual extortion of children. CSEA activity can include attempts to migrate children to a third party service for the purpose of grooming or sexually extorting a child.

See also the definitions in the Industry standards for Relevant Electronic Services regarding class 1A and class 1B material: Register of industry codes and industry standards for online safety | eSafety Commissioner

Class 1 material: Material that is, or would likely be, refused classification (**Refused Classification or RC**) by the Classification Board under the National Classification Scheme. It includes material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence, or
- advocates the doing of a terrorist act.

Class 2 material: Material that is, or would likely be, classified R 18+ or X 18+ under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old (such as pornography, and other high impact material).

Cyberbullying material targeted at an Australian child: Has the meaning given at section 6 of the Online Safety Act 2021.

End-user: A natural person who is an end-user of a product or online service.[3]

Grooming: The process of building an emotional connection with a child in order to sexually abuse or exploit them. This increasingly involves children being tricked or coerced into sexual activity on webcams or into sending sexual images through online services. Grooming is a type of CSEA activity.

Hash-matching tools: Digital technology used to create a unique digital signature (known as a 'hash') of an image or video which is then compared against signatures (hashes) of other photos to find copies of the same image or video.

Hash database: A database of material that has been previously confirmed to contain harmful and/or unlawful material. For example, the Global Internet Forum to Counter Terrorism hash-sharing database.

Language analysis tools: Technologies using methods to assign a probability that text or conversations involve certain behaviour, such as grooming a child for sexual abuse. This may involve artificial intelligence programming.

Material: Defined in section 5 of the Act to mean material, whether in the form of text, data, speech, music or other sounds, visual images (moving or otherwise), of any other form or any combination of forms. In the context of CSEA, 'material' typically refers primarily to images or video content.

Notice: A non-periodic notice given to a provider under section 56(2) of the Act on 1 April 2026.

Online hate policies: Policies relating to Roblox's Community Standards on 'Discrimination, Slurs and Hate Speech'.[4]

Recidivism: In the context of this Notice, banned or suspended users re-registering to a service with the same or new details. Multiple fake or imposter accounts may be created by a human user or by an automated bot programmed by a human.

Report period: When providers receive a reporting Notice from the eSafety Commissioner ('eSafety') they are required to prepare a report about the extent to which they complied with the Expectations during a specified period. This period is referred to as the 'report period'. The report period for this set of Notices is 1 October 2025 to 31 March 2026. Information provided reflects this period, unless stated otherwise.

Sexual extortion: A crime involving online blackmail, where victims are tricked into sending intimate images of themselves to someone who then threatens to share the images unless demands are met,

---

[3] 'Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms', 2025, accessed 18 August 2025, URL: https://onlinesafety.org.au/wp-content/uploads/2025/07/CLEAN-Phase-2-OSA-Codes-Head-Terms-1.pdf

[4] Roblox, 'Roblox Community Standards', accessed 25 February 2026, URL: Roblox Community Standards | Roblox.

usually for payment. eSafety requires information relating to any instance of sexual extortion, not only those including children. Sexual extortion is a type of CSEA activity.

Violence material and activity: Material or activity which promotes, incites or instructs in matters of crime or violence. Violence material is material which would be, or would likely be, defined as class 2 material for the purposes of section 107 of the Act, or class 1 material for the purposes of section 106 of the Act.

Violence material includes pro-terror material, crime and violence material and extreme crime and violence material as define by the Industry Standards for Relevant Electronic Services: Register of industry codes and industry standards for online safety | eSafety Commissioner. For the purposes of this notice, violence activity may include attempts to migrate children to an external platform for the purposes of sharing violence material (e.g. sharing links to a specific forum or community associated with violence material or activity).

Schedule D - Information sheet: Right of Review

Internal review by the eSafety Commissioner (eSafety)

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things:

- affirm the eSafety Commissioner's decision
- vary the eSafety Commissioner's decision; or
- set the eSafety Commissioner's decision aside and replace it with its own decision.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be waived, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

If we have not provided the reasons for this decision, you may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by eSafety under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to eSafety in writing through one of the following options:

Online: using the **Contact Us** form on eSafety's website

Email: FOi@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal or email address for us to reply to and which we can use to communicate with you about your application.

eSafety's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that eSafety has handled this matter, we ask that you contact us using the **Contact Us** form on eSafety website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with eSafety first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Unlawful and/or harmful material and activity

1. Q1. Does Roblox Corporation consider the following material and activity types to be unlawful and/or harmful?

	Choose all that apply
CSEA material and activity	☐
Violence material and activity	☐
Cyberbullying	☐
Material and activity covered by Roblox Corporation's online hate policies	☐

Section 1: Age assurance

Expectations 6(2), 6(2A), 11 and 12.

2. Q2. During the report period, did Roblox Corporation use tools and techniques to assess the age of end-users on Roblox?

    a. Yes
    b. No

If yes (a) at Q2

3. Q3. Name all the tools and techniques Roblox Corporation used to assess the age of end-users on Roblox and whether the tool or technique was an internal proprietary tool or technique, or provided by a third party.

Name of tool or technology	Internal proprietary tool or technique	Third party tool or technique
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o

If yes to third party tool at Q3

4. Q4. For each third-party tool or technique identified at Q3, specify the name of the third-party provider.

Name of tool/technology	Third party tool provider name
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	

5. Q5. For each tool listed at Q3, specify the type of tool or technique from the list below.

Name of tool/technology	Type of technology or technique used (Drop down list will be displayed with options listed below,)
(Tool from Q3 will be auto populated)	- Self declaration - Facial age estimation - ID document verification (government) - ID document verification (non government) - Credit card verification - Age inference model - Age key - Vouching (parental) - Vouching (other user or institution) - Other
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above

If Other (specify) at Q5 – (only tools where other specify were chose will appear)

6. Q5-1. Specify the 'other' type of tool or technique used.

Name of tool	Specify the type of technology used
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	

If using Age inference models at Q5.

7. Q6. For the age inference models listed in Q5, specify all the indicators that Roblox Corporation used to assess the age of end users on Roblox. (multiple response)

	Choose all that apply
Operating system indicators	☐
App store indicators	☐
Cross platform indicators	☐
Language analysis	☐
Voice analysis	☐
Image classifiers	☐
Video classifiers	☐
Device identifiers	☐
IP address indicators	☐
Traffic indicators	☐
Financial indictors	☐
Behavioural indicators (list the behavioural indicators)	☐

Other (specify)	☐
Other (specify)	☐
Other (specify)	☐

If yes (a) at Q2

8. Q7. Specify when each of the tools and techniques listed in response to Q3 were used:

	At sign up	Upon accessing certain game features or parts (eg. text chat, store or particular rooms or areas within a game)	During gameplay	To access certain Experiences;	When an account has been flagged for review by automated tools/human moderators	In response to a user report	When the service is accessed on a particular device (e.g. console, PC, mobile)	To gain access to parental controls	Other
Name of tool from Q3 will be auto populated)	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐
As above	☐	☐	☐	☐	☐	☐	☐	☐	☐

If *Upon accessing certain game features (e.g. text chat, store)* at Q7 was chosen – (Only tools where this option was chosen will appear)

9. Q7-1. Specify the 'certain game features or parts (e.g. text, chat, store or particular rooms or areas within a game)' on Roblox where the tool or technique was used.

Name of tool	Game features tool was used in
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	
(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

(Tool from Q7 will be auto populated if *Upon accessing certain game features* was chosen)	

If other (specify) was chosen for any response at Q7

10. Q7-2. Specify when the 'other' tool or technique was used on Roblox.

Name of tool	Specify
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	

If used a tool to assess the age of end-users (Yes at Q2)

11. Q8. During the report period, did Roblox Corporation or a third-party provider of a tool or technique assess the effectiveness of these tools and techniques used on Roblox?

Name of tool/technology	Yes – Roblox Corporation assessed	Yes – Third-party provider assessed	No
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○

If yes at Q8 (assessed accuracy of the tools)

12. Q9. What metrics did Roblox Corporation (or the third-party provider of a tool or technique) use to assess the effectiveness of each tool and technique? Include the specific metrics, and any relevant standards or certification schemes that Roblox Corporation relied on to evaluate the effectiveness of a tool in your answer.

Name of tool/technology	Specify the effectiveness metric used for the assessment
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

13. Q10. What was the result of the assessment for effectiveness of each tool and technique?

Name of tool/technology	Specify details of the result
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

14. Q11. What action was taken as a result of the assessment for each tool and technique?

Name of tool/technology	Specify the action taken
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

15. Q12. During the report period, what action did Roblox Corporation take after it became aware that the age information it held about an end-user may be incorrect.

	Choose all that apply
Banned account	☐
Suspended account	☐
Directed to undergo age assurance	☐
Strike against account	☐
Other (specify)	☐

IF yes at Q2

16. Q13. For the periods 1 Oct 2025 to 6 Jan 2026 and 7 Jan 2026 to 31 Mar 2026, specify how many end-users were found to be incorrectly age assured by the tools and techniques identified at Q3 to assess the age of end-users.

17. Q14. Provide any other relevant information or context in relation to your responses to questions 1 to 13, including:
    a. whether Roblox Corporation undertook any research or development work during the report period in relation to age assurance
    b. whether responses to these questions are affected by whether an end-user uses Roblox on particular devices (e.g. on a particular console, PC, or mobile)

Section 2: Staffing / Moderation

Expectations 6(2), 6(2A), 11 and 12.

18. Q15. As at 31 March 2026, provide the number of staff employed by Roblox Corporation for the below categories.

	Specify number employed
Engineers employed by Roblox Corporation who spend at least 50% of their time on trust and safety	
Content moderators employed by Roblox Corporation	
Content moderators contracted employed by Roblox Corporation	
Trust and safety staff employed by Roblox Corporation (other than engineers and content moderators)	

19. Q16. As at 31 March 2026, provide the number of moderators (contracted or employed by Roblox Corporation) trained in the following unlawful or harmful material or activity:

	Specify number of moderators trained in each following unlawful or harmful material or activity
Grooming	
Other CSEA material and activity	
Sexual extortion	
Violence material and activity	

20. Q17. As at 31 March 2026, specify which of the below languages Roblox Corporation's trust and safety staff operated in.

	Choose all that apply
English	☐
Mandarin	☐
Arabic	☐
Vietnamese	☐
Cantonese	☐
Punjabi	☐
Other languages	☐

If other (specify) was chosen for any response at Q17

21. Q18. What is the total number of the **other** languages that the Roblox Corporation's contractor trust and safety staff operated in?

Number of other languages (excluding those listed at Q17)	

22. Q19. Provide any other relevant information or context in relation to your responses to questions 15 to Q18.

Section 3: User reporting

Expectations 14(1A).

23. Q20. For the periods 1 Oct 2025 to 6 Jan 2026 and 7 Jan 2026 to 31 Mar 2026, specify the number of **global** end-user reports of unlawful or harmful material or activity on Roblox which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Global user reports between 1 Oct 2025 to 6 Jan 2026	Global user reports between 7 Jan 2026 to 31 Mar 2026
Grooming		
Sexual extortion		
Other CSEA material and activity		
Violence material and activity		
Cyber-bullying		
Material and activity covered by Roblox Corporation's online hate policies		

24. Q21. For the periods 1 Oct 2025 to 6 Jan 2026 and 7 Jan 2026 to 31 Mar 2026, specify the number of **Australian** user reports of unlawful or harmful material or activity on Roblox which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Australian user reports between 1 Oct 2025 to 6 Jan 2026	Australian user reports between 7 Jan 2026 to 31 Mar 2026
Grooming		
Sexual extortion		
Other CSEA material and activity		
Violence material and activity		
Cyber-bullying		
Material and activity covered by Roblox Corporation's online hate policies		

25. Q22. During the report period, specify the median time taken to reach an outcome after an end-user made a report, where reports were reviewed by human moderators. Provide responses for the median time concerning each of the following unlawful or harmful material or activity on Roblox.

This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review.

Provide a response in minutes

	Median time taken (minutes)
Grooming	
Sexual extortion	
Other CSEA material and activity	

Violence material and activity	
Cyber-bullying	
Material and activity covered by Roblox Corporation's online hate policies	

26. Q23. During the report period, specify the median time taken to reach an outcome after automated tools flagged potential unlawful or harmful material or activity on Roblox, where flags were reviewed by human moderators. Specify for each of the following unlawful or harmful material or activity.

    This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review

	Median time taken
Grooming	
Sexual extortion	
Other CSEA material and activity	
Violence material and activity	
Cyber-bullying	
Material and activity covered by Roblox Corporation's online hate policies	

27. Q24. For the periods 1 Oct 2025 to 6 Jan 2026 and 7 Jan 2026 to 31 Mar 2026, specify the proportion in percentage of unlawful or harmful material or activity that was detected proactively vs reported by users on Roblox, concerning the following unlawful or harmful material or activity.

	1 Oct 2025 to 6 Jan 2026		7 Jan 2026 to 31 Mar 2026	
	Detected proactively (%)	Reported by end-users (%)	Detected proactively (%)	Reported by end-users (%)
Grooming				
Sexual extortion				
Other CSEA material and activity				
Violence material and activity				
Cyber-bullying				
Material and activity covered by Roblox Corporation's online hate policies				

28. Q25. Explain how the answers to questions Q20 to Q24 were calculated and provide any other context.

	Specify how answers were calculated and provide any other context
Number of **Global** end-user reports	
Number of **Australian** end-user reports	

Median time taken to reach outcome from **Global** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from **Australian** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from automated tools that were reviewed by human moderators	
Percentage of unlawful or harmful material or activity detected proactively vs reported by users	

Section 4: Action taken against end-users

Expectations 14(1A) and 14(2)

28. Q26. During the report period, what action did Roblox Corporation take after an end-user breached the terms of service and/or community guidelines (or equivalent) in relation to the following unlawful or harmful material or activity.

	Sexual extortion	Grooming	Other CSEA material and activity		Violence material and activity	Cyberbullying	Conduct that breaches Roblox Corporation's online hate policies
Banned account	☐	☐	☐		☐	☐	☐
Suspended account	☐	☐	☐		☐	☐	☐
Strike/Warning given to end-user	☐	☐	☐		☐	☐	☐
Restricted player's access to certain features of the game (e.g. ability to interact with other players)	☐	☐	☐		☐	☐	☐
Removed harmful content created by user (e.g. user-generated content, messages)	☐	☐	☐		☐	☐	☐
Prevented user from creating certain content (e.g. marketplace items)	☐	☐	☐		☐	☐	☐
Other (specify)	☐		☐	☐	☐	☐	☐

29. Q27. During the report period, were Roblox Corporation's trust and safety staff automatically informed when Roblox Creators banned an account from their Experience for behaviour related to the following unlawful or harmful material or activity.

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Other CSEA material and activity	o	o
Violence material and activity	o	o
Material and activity covered by Roblox Corporation's online hate policies	o	o

If trust and safety were not informed automatically at Q27 – No to at least 1.

30. Q28. How did Roblox Corporation ensure that a user banned from an Experience for breaches related to the unlawful or harmful material or activity at Q27 was not able to engage in this activity on other parts of the service?

Q29. Provide any other relevant information or context in relation to your responses to questions 26 to 28, including whether responses to these questions are affected by whether an end-user uses a particular edition/model of Roblox or uses Roblox on particular devices (e.g. on a particular console, PC, or mobile)

Section 5: Tools and Techniques

Expectations 6(2), 6(2A), 11 and 12.

31. Q30. During the report period, did Roblox Corporation use tools and/or techniques on Roblox to detect the following unlawful or harmful material or activity?

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Other CSEA material and activity	o	o
Violence material and activity	o	o
Attempts to migrate children to another service	o	o

If used tool/techniques to identify harms (Yes for any at Q30)

32. Q31. Name all the tools and techniques used and which harm types they cover.

	Grooming [IF yes to Grooming at Q29]	Sexual extortion [IF yes to Sexual extortion at Q29]	Other CSEA material and activity [IF yes to Other CSEA at Q29]	Violence material and activity [IF yes to Violence at Q29]	Attempts to migrate children to another service [IF yes to

					attempts to migrate at Q29]
Tool 1 (Specify)	☐	☐	☐	☐	☐
Tool 2 (Specify)	☐	☐	☐	☐	☐
Tool 3 (Specify)	☐	☐	☐	☐	☐
Tool 4 (Specify)	☐	☐	☐	☐	☐
Tool 5 (Specify)	☐	☐	☐	☐	☐
Tool 6 (Specify)	☐	☐	☐	☐	☐
Tool 7 (Specify)	☐	☐	☐	☐	☐
Tool 8 (Specify)	☐	☐	☐	☐	☐
Tool 9 (Specify)	☐	☐	☐	☐	☐
Tool 10 (Specify)	☐	☐	☐	☐	☐

If used tool/techniques to identify violence material or violence activity at Q31

33. Q32. Specify the types of 'violence material and/or activity' the tool/technique is used to identify.

	Specify below
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	

If used tool/techniques to identify harms (Yes for any at Q30)

34. Q33. For each tool and technique identified at Q31, specify which part of the service it is used on.

[Roblox response options]	Experiences	Interactions between avatars	Direct Experience chat	Experience text chat	Experience voice chat	Party text chat	Party voice chat	Catalogue/ library items (e.g. clothing, text on clothing/ accessories, emotes)		Other (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

IF other at Q33

36. Q33-1. Specify the 'other' part of the service where the tool or technique was used.

	Specify
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

36. Q34. For each tool and technique identified at Q31, specify the type of tool or technique.

	Language analysis tool (text) `	Language analysis tool (audio)	AI classifier	Hash-matching tool	Signals-based detection (e.g. behavioural indicators, financial indicators (specify)	Other (e.g. detecting URL join links) (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐

If Other (specify) chosen for any tool at Q34.

37. Q34-1. Specify the other type of tool or technique for each tool.

Name of tool	Specify

(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

If Signals-based detection (specify) chosen for any tool at Q34.

38. Q35. Specify the signals used for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

39. Q36. For each tool or technique identified Q31, specify whether the tool detects material before or after it is published (i.e. as part of a pre-screening process).

	Before material is published	After material is published	Provide any relevant details
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	

If used hash-matching tool at Q34

40. Q37. For each hash-matching tool identified at Q34, specify the names of the hash-matching source databases used.

Choose all that apply.

	GIFCT	IWF	NCMEC	Other (specify)
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	

(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	

Q37-1. Please specify the 'other' hash-matching source database for the tools below.

	Other (specify)
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

41. Q38. For each hash-matching tool identified at Q34, specify the frequency at which Roblox Corporation updated the hashes it scanned on Roblox against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (Specify)
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○
(Hash-matching tool from	○	○	○	○	○	○

Q34 will auto populate)						
(Hash-matching tool from Q34 will auto populate)	○	○	○	○	○	○

41. Q38-1. Specify the 'other' frequency at which Roblox Corporation updated the hashes it scanned on Roblox against these databases.

	Specify
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

IF used language analysis tool at Q34

42. Q39. For each language analysis tool identified at Q34, specify all the languages it operated in.

Choose all that apply.

	English	Mandarin	Arabic	Vietnamese	Cantonese	Punjabi	Other	Language agnostic
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐

If other (specify) was chosen for any response at Q39

43. Q40. What is the total number of **other** languages that the language analysis tool operated in?

Number of other languages (excluding those listed at Q39)	

If use language analysis tool at Q34

44. Q41. For each language analysis tool identified at Q34, specify whether the tool has been trained to do any of the following:

	Key-word detection	Interpret sentence level context	Interpret conversation-level context	Distinguish joking/irony from serious intent	Interpret coded or indirect language (including use of emojis or symbols in words)	Interpret formatting or hashtags as context clues	Detect coercive or manipulative language	Detect attempts to migrate children to another service	Provide any other relevant details
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	

If tool used language analysis tools at Q34

45. Q42. List all the organisations used to source keywords/training data for the language analysis tools listed below.

	GIFCT	IWF	NCMEC	Lantern	Other (specify)

(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	

IF other at Q42

45. Q42-1. Provide details on the other organisations used to source keyword/training data for the language analysis tools.

	Other (specify)
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	

If tool used language analysis tools at Q34

46. Q43. For each language analysis tool identified at Q34, specify the frequency Roblox Corporation updated the tool against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (specify)
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool from Q34 will auto populate)	○	○	○	○	○	○
(Language analysis tool	○	○	○	○	○	○

from Q34 will auto populate)						
(Language analysis tool from Q34 will auto populate)	o	o	o	o	o	o

IF other at Q43

46. Q43-1. Provide details on the frequency that Roblox Corporation updated the language analysis tools against the source keyword/training data.

47. ASK ALL who use tools Q33 yesQ44. During the report period, did Roblox Corporation assess the accuracy of all the below tools used to detect the unlawful or harmful material or activity?

	Yes	No
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o

If assessed accuracy of tools (Yes at Q44)

48. Q45. Provide details of the assessment methodology, specify details of any red teaming or simulated adversarial testing.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

49. Q46. What were the results of this assessment? Include **precision** and **recall rates** in your answer, and/or **any other metrics used to quantify the result**, with relevant context.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

50. Q47. What action was taken as a result of the assessment for each tool?

	Specify action taken
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

51. Q48. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **Grooming**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Grooming at Q48.

57. Q48-1. If only in certain circumstances for Grooming, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	

53. Q49. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **sexual extortion**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o

(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for sexual extortion at Q49

57. Q49-1. If only in certain circumstances for sexual extortion, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	

54. Q50. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **other CSEA material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Other CSEA at Q50

57. Q50-1. If only in certain circumstances for other CSEA material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	

55. Q51. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **violence material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for violence material and activity at Q51

57. Q51-1. If only in certain circumstances for violence material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	

56. Q52. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances **on attempts to migrate children to another service**?

	Used on all material by default	Used on material in some circumstance
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for attempts to migrate children at Q52

57. Q52-1. If only in certain circumstances on attempts to migrate children to another service, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q52 that are used in some circumstances will auto populate)	

(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	

58. Q53. During the report period, did Roblox Corporation take steps to identify an Experience which may be higher risk for grooming, sexual extortion, other CSEA material and activity, violence material and activity and/or material and activity captured by Roblox Corporation's online hate policies? Y/N

If Yes at Q53

59. Q54. Specify any measures used by Roblox Corporation, in addition to the tools and techniques identified at Q31 to address grooming, sexual extortion, other CSEA material and activity, violence material and activity and online hate policies on these higher risk Experiences.

60. Q55. During the report period, did Roblox Corporation use any tools or other measures to detect transactions of Robux and/or Robux gift cards that may be linked to grooming and/or sexual extortion?

    1. Yes (specify details)
    2. No

61. Q56. Specify the details of the tools or other measures used to detect transactions of Robux and Robux gift cards that may be linked to grooming and/or sexual extortion.

62. Q57. Provide any other relevant information or context in relation to your responses to questions 39 to 46, including:
    a. whether Roblox Corporation undertook any research or development work during the report period in relation to proactive detection of the harms listed in Q30
    b. whether responses to these questions are affected by whether an end-user uses Roblox on particular devices (e.g. on a particular console, PC, or mobile)

Section 6: Recidivism

Expectations 14(1A).

63. Q58. During the report period, did Roblox Corporation use the below indicators to identify recidivism after an end user had been banned or suspended for CSEA or violence material and activity.

	CSEA	Sexual extortion	Violence material and activity
Device identifiers	☐	☐	☐
Phone number	☐	☐	☐
Behavioural indicators	☐	☐	☐
Email address	☐	☐	☐
Geographical indicators	☐	☐	☐
Financial indicators	☐	☐	☐
Profile picture	☐	☐	☐
Username	☐	☐	☐
Name	☐	☐	☐
Date of birth	☐	☐	☐
Display name	☐	☐	☐
Other (specify)	☐	☐	☐
Other (specify)	☐	☐	☐

If used indicators to identify recidivism at Q58.

64. Q59. Were indicators used by default in all cases where an account has been banned or suspended for **CSEA material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

65. Q60. Were indicators used by default in all cases where an account has been banned or suspended for **sexual extortion**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

66. Q61. Were indicators used by default in all cases where an account has been banned or suspended for **violence material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

If used indicators to identify recidivism at Q58.

67. Q62. What specific action did Roblox Corporation take based on these indicators? If the action taken differed based on the specific indicators, specify all those differences, e.g. automatically blocked accounts with these indicators from being created; flagged the account for human review etc.

	Specify action taken
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	

68. Q63. Provide any other relevant information or context in relation to your responses to questions 58 to 62 including:
    a. whether Roblox Corporation undertook any research or development work during the report period in relation to prevention of recidivism on Roblox
    b. whether responses to these questions are affected by whether an end-user uses Roblox on particular devices (e.g. on a particular console, PC, or mobile)

Section 7: Moderation of user-generated content

Expectations 14(1A).

69. Q64. During the report period, did Roblox take any action to detect and remove any of the following unofficial developer-built chat functions (outside of Roblox's standard Text/Voice Chat functions)?

	Choose all that apply
Unofficial text chat functions	☐
Unofficial voice chat functions	☐

[Roblox only] If had measures in place at Q48a

70. Q65. What actions did Roblox Corporation take against Creators with unofficial chat functions in their Experiences?

	Choose all that apply
Disabled chat feature within Experience	☐
Banned Experience	☐
Banned Creator	☐
Suspended Creator	☐

Other (specify)	☐

Section 8: Information sharing initiatives

Expectations 10(1) and 14(1A).

70. Q66. During the report period, did Roblox Corporation share information with the following services or initiatives (including bi-lateral arrangements with other providers) for the purpose of minimising grooming/sexual extortion and violence material and activity on its service?

	Choose all that apply
Lantern	☐
Tech Coalition	☐
Fair Play Alliance	☐
Tech Against Terrorism	☐
Discord	☐
Twitch	☐
Steam	☐
Other Initiatives/Services (specify)	☐

If a member of information sharing initiative (any at Q66)

71. Q67. Explain the steps taken as a result of sharing information with the below initiatives.

	Specify steps taken
(Auto populate sharing initiative chosen at Q669)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	

72. Q68. Provide any other relevant information or context in relation to your responses to questions 66 to 67, including whether Roblox Corporation undertook any research or development work during the report period in relation to collaborating with civil society organisations or other service providers to prevent harm on Roblox

Section 9: Off-platform monitoring

Expectations 6(2), 6(2A), 11 and 12.

73. Q69. During the report period, did Roblox Corporation use off-platform monitoring (monitoring of activity on other services either provided internally or by third-party services) to identify accounts or communities present on its service that are engaged in the below harms.

	Yes	No

Grooming	o	o
Sexual extortion	o	o
Violence activity	o	o

If used off-platform monitoring (Yes at Q69)

74. Q70. Provide details, specifying what this involved and what third party services were used.

	Specify details	Specify names of third parties used
Grooming		
Sexual extortion		
Violence activity		

75. Q71. Provide any other relevant information or context in relation to your responses to Q69 and Q70 , including whether Roblox Corporation undertook any research or development work during the report period in relation to monitoring of other services to identify accounts or communities engaged in the harms listed at Q69.

Section 10: Other

Expectations 6(2), 6(2A) and 11.

76. Q72. During the report period, did Roblox Corporation provide any help services or support to users who were identified as potential victims of grooming and/or sexual extortion?
    a. Yes
    b. No

IF yes at Q53

77. Q73. Provide details on the help services or support Roblox Corporation provided to users who were identified as potential victims of grooming and/or sexual extortion.

78. Q74. As at 31 March 2026, specify the proportion of under 18 accounts in Australia that have parental supervision enabled.

79. Q75. Explain how the answer to Q74 was calculated and provide any other context, including whether the use of parental controls on Roblox are affected by whether an end-user uses Roblox on particular devices (e.g. on a particular console, PC, or mobile).

Section 11: Final question

80. Q78. Outline any further steps Roblox Corporation is taking to meet Expectations 6(2), 6(2A), 10(1), 11, 12, 14(1A) and 14(2).

    Do not replicate information provided in previous responses here. This is an opportunity for Roblox Corporation to outline information about other types of safety measures.

1 April 2026

Our reference: BOSE-2026-104

Valve Corporation

c/o s 47F Valve Corporation

By email: s 47F @valvesoftware.com; cc s 47F @valvesoftware.com

Dear s 47F

Non-periodic reporting notice requiring Valve Corporation to prepare a report about the extent to which it has complied with the Basic Online Safety Expectations

The eSafety Commissioner is responsible for improving and promoting online safety for Australians. This includes giving notices to service providers about their compliance with the Basic Online Safety Expectations (**the Expectations**), and publishing summaries of our findings. For more information about eSafety's role and functions, please refer to our website.

The publication of findings serves to increase the transparency and accountability of online services in demonstrating the actions that they are taking to protect Australians from harms online. Transparency also empowers Australians with information to better understand the online environment and any safety risks that may be present on services.

By highlighting what we have learned from notices, eSafety's aim is that the information is also used by researchers, academics, the media and the public to scrutinise the efforts of industry to encourage implementation of the Expectations and to lift safety practices, protections and standards across the industry.

Please see enclosed a non-periodic reporting notice (**the Notice**) given to Valve Corporation (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**). The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Basic Online Safety Expectations during the period specified in the Notice in respect to the Steam service and the Steam Chat service (**the Services**).

The Notice requires the Provider to give the report to the Commissioner by **17:00 Australian Eastern Standard Time (AEST) on 11 May 2026.**

If you require additional time to comply with the Notice, you may request this by sending an email to industryBOSE@esafety.gov.au before 17:00 AEST on 27 April 2026.

The manner and form of the required report are included in **Schedule B** to the Notice. Instructions on this requirement are included in the Notice. Definitions of relevant terms are included in **Schedule C** to the Notice.

The specified applicable Basic Online Safety Expectations

The Notice focuses on the steps being taken to comply with the basic Expectations, with a focus on the following unlawful and/or harmful material and activity:

a. is child sexual exploitation and abuse (CSEA);

b. promotes, incites or instructs in matters of violence;

c. is cyberbullying; and

d. falls under:

i. the Provider's rules and guidelines for 'Steam discussions, reviews and user generated content', specifically the portions of the guidelines relating to disrespectful content including discrimination, encouraging or facilitating real-world violence, directing abuse or insults at others or using content to harass, abuse or otherwise disparage others, or uploading inappropriate content

ii. portions of Steam's Online Code of Conduct which relate to engagement in unlawful activity, uploading or posting illegal or inappropriate content, violating others' personal rights, or harassing other users or Steam personnel.[1]

The Expectations are contained in the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth), which commenced on 24 January 2022. The relevant regulatory guidance is available here.

What you are required to report on

See **Schedule A** for full details of the specific expectations that, under the Notice, the Provider is required to report on.

The decision to give the Notice

I have decided to give the Notice under section 56(2) of the Act. In deciding whether to give a non-periodic reporting notice, I am required by section 56(5) of the Act to have regard to the following criteria, against which I have summarised my considerations:

a) The number of occasions during the previous 12 months on which complaints about material provided on the Service were made to the Commissioner under the Act:
   - During the period 20 March 2025 to 20 March 2026, the eSafety Investigations Branch received 63 complaints relating to material available on the Services, including 4 complaints relating to cyberbullying material; 2 relating to Imaged based abuse; and 49 relating to illegal and restricted content.
   - I do not rely on this factor as a reason for giving this Notice.

[1] Valve Corporation, 'Rules and guidelines for Steam discussions, reviews and user generated content', accessed 2 February 2026, URL: Steam Support :: Rules and Guidelines For Steam: Discussions, Reviews, and User Generated Content; Valve Corporation, 'Steam Online Conduct', accessed 26 March 2026, Steam Online Conduct.

b) Whether the provider has previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act:
    - The Provider has not previously contravened a civil penalty provision of Division 3 (Reporting), Part 4 of the Act. I do not rely on this factor as a reason for giving this Notice.

c) Whether there are deficiencies in the Provider's practices, so far as they relate to the capacity of end-users to use the services in a safe manner:
    - I note reports from expert agency, research and media reports relating to the potential for unlawful and/or harmful material or activity on the Services, as well as harms associated with online gaming services, particularly as they relate to children.
    - I consider that these reports indicate a risk that Australians, especially Australian children, may be exposed to unlawful or harmful material or activity on the Services. The Notice would assist me in understanding what steps the Provider is taking to comply with Expectations 6(2) and 6(2A).

d) Whether there are deficiencies in the services' terms of use, so far as they relate to the capacity of end-users to use the services in a safe manner:
    - I consider the Notice would assist me in understanding the steps the Provider is taking to enforce its terms of service and comply with Expectations 6(2), 6(2A) and 14(1A) of the Determination.

e) Whether the provider has agreed to give the Secretary regular reports relating to the capacity of end users to use the service in a safe manner;
    - There is no ongoing agreement between the Provider and the Secretary of the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts for regular reports for the purpose of section 56(5)(e). As such, I consider the Notice to be of assistance to exercising my statutory functions.

f) Such other matters (if any) as the Commissioner considers relevant.
    - As well as the considerations above:
        - I consider the use of the Services by Australians to be a risk factor as any failure to comply with the relevant Basic Online Safety Expectations puts Australians at risk, including children.
        - I consider that the Services' features such as its instant messaging chat functions and discussion boards which enable interaction between children and adults, ability to create user-generated content, the availability of in-service trading of online items are high-risk features with the potential to increase the risk of CSEA activity (e.g. grooming and sexual extortion) and violence material and activity (e.g. youth radicalisation) if appropriate safeguards are not put in place by the Provider.
    - I consider that the following, but not limited to, information gaps limit eSafety's understanding of the steps the Provider is taking to ensure safe use and proactively minimise harmful content such as CSEA, violence material and cyberbullying on the Services:
        - Quality of training data and effectiveness of moderation tools;
        - Information on content moderators;
        - Information sharing with other providers;
        - Measures to address recidivism;

Additionally, giving the Notice supports my statutory functions as set out in section 27 of the Act, including to promote online safety for Australians, to monitor compliance with the Act, and to collect, analyse, interpret and disseminate information relating to online safety for Australians.

Required action

The Notice requires the Provider to prepare a report, in the manner and form specified, about the extent to which it complied with the specified applicable Expectations during the period specified in the Notice and give the report to the Commissioner by **17:00 AEST on 11 May 2026.**

Failure to comply with the Notice may result in the Commissioner taking enforcement or compliance action.

You should contact eSafety prior to the Notice deadline if any of the following apply, and take the steps indicated:

- You consider that a question does not apply to your service(s). Provide reasons and an explanation of why the question does not apply.
- You consider that you are not capable of answering a question. Identify the question(s) and provide reasons and an explanation of why you are not capable of answering the question(s). eSafety will consider your reasons and explanation and advise on an appropriate course of action.
- You require additional time to comply with the Notice and to provide the required information. You must request an extension of time from eSafety and provide specific reasons why you are not capable of meeting the deadline specified in the Notice. eSafety will inform you if an extension of time has been granted by the Commissioner.
- You would like to request an alternative means of returning Schedule B to the Notice other than via Qualtrics. Provide reasons and suggest an alternative method of providing the information. eSafety will arrange appropriate alternate means where appropriate.

eSafety will engage with all providers who contact eSafety. We request that you comply with the instructions given by eSafety in response to any of the above requests.

Extension of time to comply

If the Provider requires additional time to comply with the Notice, please email industryBOSE@esafety.gov.au before **17:00 AEST on 27 April 2026.** In your email, please include reasons for your request.

You may seek an extension of time any time before **17:00 AEST on 27 April 2026**. If you submit a request for an extension of time less than 2 weeks prior to **17:00 AEST on 11 May 2026**, you should include reasons as to why an extension was not sought earlier, as well as reasons for the request.

The deadline in the Notice continues to apply unless eSafety confirms that an extension is granted.

Failure to comply

Under section 57 of the Act, the Provider must comply with the requirement under the Notice to the extent that it is capable of doing so.

Failure to comply with the Notice is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate, following the end of the period

specified for compliance with the Notice. eSafety also has a range of other enforcement options, as detailed in the regulatory guidance.

False or misleading information or documents

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to eSafety or the eSafety Commissioner.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Review rights

The Provider has a right to seek an internal or external review of the decision to give a notice to it under section 56(2) of the Act.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

More detailed information about the Provider's review rights is available in the information sheet at Schedule D to this correspondence which sets out the Provider's rights with respect to the different review options available to it, as well as other options if you do not agree with the decision to give the Notice to the Provider.

Confidentiality

eSafety intends to publish a summary of the Provider's responses to the Notice, pursuant to section 217 of the Act. Part of the purpose of collecting the information required under the Notice is publication of that information.

The Provider can make submissions about confidentiality and/or the sensitivity of information provided to eSafety. eSafety will carefully consider any objections when deciding what information to publish. Attachment A to this correspondence outlines the criteria that eSafety will have regard to in considering confidentiality submissions.

The Provider must provide the information required by the Notice even if you have concerns about confidentiality and/or sensitivity of certain information and make submissions to eSafety about the publication of confidential and sensitive information.

eSafety will prepare a summary of information for publication. Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, the Provider will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.

Regards,



Julie Inman Grant
eSafety Commissioner

Enclosed: Notice under section 56(2) of the Act

Information Sheet: Review Rights

NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Valve Corporation (the **Provider**)

Attention: s 47F Valve Corporation

By Email: s 47F @valvesoftware.com; cc s 47F @valvesoftware.com

This non-periodic reporting notice (**Notice**) is given to Valve Corporation (the **Provider**) under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) in respect of the Steam service and the Steam Chat service (the **Services**) that it provides in Australia.

The Provider is required to prepare a report about the extent to which it complied with the applicable Basic Online Safety Expectations specified in **Schedule A** for the period 1 October 2025 to 31 March 2026 inclusive (**Report Period**).

The Provider is required to provide the report in the manner and form specified in **Schedule B,** including following the instructions provided, and answering the questions included in **Schedule B.**

The Provider is required to give the report to the Commissioner within 40 days of being given this Notice, being no later than **17:00 AEST on 11 May 2026** (the **Due Date**), or within such longer period as the Commissioner allows if the Commissioner is contacted by the Provider with a request for an extension of time.

The report is to be given to the Commissioner via the Qualtrics report form in Schedule B of the Notice.

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of AUD$825,000 each day for a single contravention by a body corporate.

It is an offence under the *Criminal Code Act 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Date: 1 April 2026



Julie Inman Grant

eSafety Commissioner

Schedule A – specified applicable Basic Online Safety Expectations

The Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) (**Determination**) commenced on 24 January 2022 and contains the Basic Online Safety Expectations, some of which Valve Corporation (the **Provider**) as the provider of the Steam service and the Steam Chat service (the **Services**), is being required to report on under this Notice. The amendments to the Determination made by the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth) came into effect on 31 May 2024.

This Schedule sets out the specified applicable Basic Online Safety Expectations to be reported on by the Provider for the purpose of this Notice:

Expectations:

6 Expectations—provider will take reasonable steps to ensure safe use

Additional expectation

(2) The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful.

Additional expectation

(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

10 Additional expectation—provider will consult and cooperate with other service providers to promote safe use

Additional expectation

(1) The provider of the service will take reasonable steps to:

(a) consult and cooperate with providers of other services; and

(b) ensure consultation and cooperation occurs between all relevant services provided by that provider, in order to promote the ability of end-users to use all of those services in a safe manner.

11 Core expectation—provider will take reasonable steps to minimise provision of certain material

The provider of the service will take reasonable steps to minimise the extent to which the following material is provided on the service:

(a) cyber-bullying material targeted at an Australian child;

(b) cyber-abuse material targeted at an Australian adult;

(c) a non-consensual intimate image of a person;

(d) class 1 material;

(e) material that promotes abhorrent violent conduct;

(f) material that incites abhorrent violent conduct;

(g) material that instructs in abhorrent violent conduct;

(h) material that depicts abhorrent violent conduct.

12 Core expectation—provider will take reasonable steps to prevent access by children to class 2 material

Core expectation

(1) The provider of the service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

14 Additional expectations—provider will ensure service has terms of use, certain policies etc.

(1A) The provider of the service will take reasonable steps (including proactive steps) to detect breaches of its terms of use and, where applicable, breaches of policies and procedures in relation to the safety of end-users, and standards of conduct for end-users.

(2) The provider of the service will take reasonable steps (including proactive steps) to ensure that any penalties specified for breaches of its terms of use, policies and procedures in relation to the safety of end-users, and standards of conduct for end-users, are enforced against all accounts held or created by the end-user who breached the terms of use and, where applicable, breached the policies and procedures, and standards of conduct, of the service.

Schedule B – link to Qualtrics form[2]

This report form constitutes Schedule B to the Notice. It specifies the manner and form of the report required by the Notice and requires you to respond to the questions included within, which relate to the Provider's compliance with the applicable Basic Online Safety Expectations. The relevant expectations are stated alongside each question.

Each of the following is a requirement under the Notice:

- Answer each question truthfully and accurately. Other information provided to the eSafety Commissioner ('eSafety') in relation to the Notice, including statements about a provider's capability to respond to the Notice and submissions related to confidentiality or sensitivity of information, must also be truthful and accurate.
- Use this report form for your response. Responding in an alternative way without prior agreement with eSafety may amount to non-compliance with the Notice.
- Provide a response to each question, and its parts unless the report form states otherwise. Leaving a response blank without providing eSafety with a reasonable explanation in advance of the deadline for the Notice (or any valid extension of time) is likely to be considered non-compliance with the Notice.
- Provide information for the period from 1 October 2025 to 31 March 2026 (**the Report Period**), unless a question requires information on a specific time period within the Report Period. Some questions may require information as at a specified date. The use of this date within the Report Period ensures that eSafety can obtain up to date information on providers' current practices and aims to reduce the burden on providers.

Navigating through the report form:

- The report form includes single and multiple response options as well as text field options.
- All text fields allow for the available window space to be increased by clicking and dragging the right bottom corner of the box and re-sizing as required.
- A Table of Contents is provided at the top left-hand side to allow for easy navigation though the questions. The forward and back buttons will allow for navigation to any question.
- A response to a question may result in subsequent questions no longer requiring a response. All questions to the report form are displayed, regardless of whether a response is required. This is to provide transparency of the full set of questions.
- Some questions are Provider specific and where there is a question for a different Provider, a note is included to note that the question has been skipped.

---

[2] Link to Qualtrics form – https://esafetydxm.qualtrics.com/jfe/form/SV_9traCr0DRCfIGKW?Q_CHL=gl&Q_DL=EMD_3dsuwk80bOEmzg4_9traCr0DRCfIGKW_CGC_C84GNPXANfT1BLi&_g_=g

- Responses are automatically saved in draft and can be revisited over the course of multiple sittings.
- Before submitting the responses, you are required to review all questions to ensure responses are provided.
- Once the report form is submitted, no further changes can be made. You may contact eSafety to reopen a submitted response before the Due Date.
- Once responses are submitted there will be a summary page with an option to download a copy of your responses to a PDF document.

Also note the following:

- Include as much information as is necessary to provide a fulsome response to the question. Question 78 is an opportunity for you to provide information as part of your report about any further safety measures the Provider is taking to comply with these specified expectations.
- You can raise concerns about confidentiality and/or the sensitivity of information. eSafety will carefully consider your submissions when deciding what information to publish. Attachment A has been provided to you to outline the criteria that eSafety will have regard to in considering confidentiality submissions. However, concerns about the confidentiality and sensitivity of certain information are not adequate reasons to refuse to provide information required by the Notice. eSafety will prepare a summary of information for publication based on the Provider's responses.
- Submissions about confidentiality and sensitivity of information will be considered by eSafety when preparing that summary. Before eSafety publishes or publicly discloses that summary, you will be given an additional opportunity to make submissions about the information that eSafety proposes to publish.
- **Definitions of relevant terms are included in Schedule C to the Notice.** If you have any concerns about the relevant terms, contact us at industryBOSE@safety.gov.au to discuss.
- Further information can also be found in the Basic Online Safety Expectations Regulatory Guidance and on the relevant page on eSafety's website.
- You can contact industryBOSE@safety.gov.au regarding any of the above information, or with any other questions about your response.
- On the final page where the 'submit' button is displayed, the following text will be included:

  This is the final page of Schedule B to the Notice. Please review your responses. Once you click 'submit', your response will be received by eSafety and all information provided is considered the Provider's response to the Notice. Note that you cannot edit your response after you click 'submit'.

Schedule C – Definitions of relevant terms

The Act: *The Online Safety Act 2021* (Cth).

Age assurance: An umbrella term which includes age verification (determining a person's age to a high level of accuracy, such as through the use of identity documents) age estimation (providing an approximate age through analysis of biological or behavioural human features that vary with age, for example through the use of facial or voice analysis), or age inference (using information other than a date of birth which indirectly implies a certain age or age range).

Child sexual exploitation and abuse (CSEA): is material or activity which includes both:

- 'child sexual exploitation' (a broad category that encompasses material and activity that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse)
- 'child sexual abuse' (which involves a sexual assault against a child, is a narrower category and can be considered a sub-set of child sexual exploitation).

CSEA material is a subset of class 1 material, as defined under section 106 of the Act by reference to the National Classification Scheme, and includes images video and text. CSEA material includes user generated content.

CSEA activity refers to other illegal activity, including grooming and sexual extortion of children. CSEA activity can include attempts to migrate children to an external platform for the purpose of grooming or sexually extorting a child.

See also the definitions in the Industry standards for Relevant Electronic Services regarding class 1A and class 1B material Register of industry codes and industry standards for online safety | eSafety Commissioner

Class 1 material: Material that is, or would likely be, refused classification (**Refused Classification or RC**) by the Classification Board under the National Classification Scheme. It includes material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence, or
- advocates the doing of a terrorist act.

Class 2 material: Class 2 material is material that is, or would likely be, classified R 18+ or X 18+ under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old (such as pornography, and other high impact material).

Cyberbullying material targeted at an Australian child: has the meaning given at section 6 of the Online Safety Act 2021.

End-user: a natural person who is an end-user of a product or online service.[3]

Grooming: The process of building an emotional connection with a child in order to sexually abuse or exploit them. This increasingly involves children being tricked or coerced into sexual activity on webcams or into sending sexual images through online services. Grooming is a type of CSEA activity.

Hash-matching tools: Digital technology used to create a unique digital signature (known as a 'hash') of an image or video which is then compared against signatures (hashes) of other photos to find copies of the same image or video.

Hash database: a database of material that has been previously confirmed to contain harmful and/or unlawful material. For example, databases provided by National Center for Missing & Exploited Children and Internet Watch Foundation for CSEA and Global Internet Forum to Counter Terrorism for violence material.

Language analysis tools: Technologies using methods to assign a probability that text or conversations involve certain behaviour, such as grooming a child for sexual abuse. This may involve artificial intelligence programming.

Material: Defined in section 5 of the Act to mean material, whether in the form of text, data, speech, music or other sounds, visual images (moving or otherwise), of any other form or any combination of forms. In the context of CSEA, 'material' typically refers primarily to images or video content.

Notice: For the purpose of this report, a Notice is a non-periodic notice given to a provider under section 56(2) of the Act on 1 April 2026.

Online hate policies: Policies relating to:

- the Provider's rules and guidelines for 'Steam discussions, reviews and user generated content', specifically the portions of the guidelines relating to disrespectful content including discrimination, encouraging or facilitating real-world violence, directing abuse or insults at others or using content to harass, abuse or otherwise disparage others, or uploading inappropriate content, and
- portions of Steam's Online Code of Conduct which relate to engagement in unlawful activity, uploading or posting illegal or inappropriate content, violating others' personal rights, or harassing other users or Steam personnel.[4]

[3] 'Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms', 2025, accessed 18 August 2025, URL: https://onlinesafety.org.au/wp-content/uploads/2025/07/CLEAN-Phase-2-OSA-Codes-Head-Terms-1.pdf

[4] Valve Corporation, 'Rules and guidelines for Steam discussions, reviews and user generated content', accessed 2 February 2026, URL: Steam Support :: Rules and Guidelines For Steam: Discussions,

Recidivism: In the context of this Notice, banned or suspended users re-registering to a service with new details. Multiple fake or imposter accounts may be created by a human user or by an automated bot programmed by a human.

Report period: When providers receive a reporting Notice from the eSafety Commissioner ('eSafety') they are required to prepare a report about the extent to which they complied with the Expectations during a specified period. This period is referred to as the 'report period'. The report period for this set of Notices is 1 October 2025 to 31 March 2026. Information provided reflects this period, unless stated otherwise.

Sexual extortion: A crime involving online blackmail, where victims are tricked into sending intimate images of themselves to someone who then threatens to share the images unless demands are met, usually for payment. eSafety requires information relating to any instance of sexual extortion, not only those including children. Sexual extortion is a type of CSEA activity.

Violence material and activity: Material or activity which promotes, incites or instructs in matters of crime or violence. For the purposes of a gaming service, examples may include:

Violence material is material which would be, or would likely be, defined as class 2 material for the purposes of section 107 of the Act, or class 1 material for the purposes of section 106 of the Act.

Violence material includes pro-terror material, crime and violence material and extreme crime and violence material as define by the Industry Standards for Relevant Electronic Services Register of industry codes and industry standards for online safety | eSafety Commissioner/. For the purposes of this notice, violence activity may include attempts to migrate children to an external platform for the purposes of sharing violence material (e.g. sharing links to a specific forum or community associated with violence material or activity).

Reviews, and User Generated Content; Valve Corporation, 'Steam Online Conduct', accessed 26 March 2026, Steam Online Conduct.

Schedule D - Information sheet: Right of Review

Internal review by the eSafety Commissioner

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things:

- affirm the eSafety Commissioner's decision
- vary the eSafety Commissioner's decision; or
- set the eSafety Commissioner's decision aside and replace it with its own decision.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be waived, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

If we have not provided the reasons for this decision, you may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online:	using the **Contact Us** form on the eSafety Commissioner's website
Email:	FOI@esafety.gov.au
Post:	**Attention:** The FOI Coordinator eSafety Commissioner PO Box Q500 Queen Victoria Building NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal or email address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Unlawful and/or harmful material and activity

1. Q1. Does Valve Corporation consider the following material and activity types to be unlawful and/or harmful?

	Choose all that apply
CSEA material and activity	☐
Violence material and activity	☐
Cyberbullying	☐
Material and activity covered by Valve Corporation's online hate policies	☐

Section 1: Age assurance

Expectations 6(2), 6(2A), 11 and 12.

2. Q2. During the report period, did Valve Corporation use tools and techniques to assess the age of end-users on Steam and Steam Chat?

    a. Yes
    b. No

If yes (a) at Q2

3. Q3. Name all the tools and techniques Valve Corporation used to assess the age of end-users on Steam and Steam Chat and whether the tool or technique was an internal proprietary tool or technique, or provided by a third party.

Name of tool or technology	Internal proprietary tool or technique	Third party tool or technique
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o
(Specify)	o	o

If yes to third party tool at Q3

4. Q4. For each third-party tool or technique identified at Q3, specify the name of the third-party provider.

Name of tool/technology	Third party tool provider name
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	
(Tool from Q3 will be auto populated)	

5. Q5. For each tool listed at Q3, specify the type of tool or technique from the list below.

Name of tool/technology	Type of technology or technique used (Drop down list will be displayed with options listed below,)
(Tool from Q3 will be auto populated)	- Self declaration - Facial age estimation - ID document verification (government) - ID document verification (non government) - Credit card verification - Age inference model - Age key - Vouching (parental) - Vouching (other user or institution) - Other
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above
(Tool from Q3 will be auto populated)	Drop down list as above

If Other (specify) at Q5 – (only tools where other specify were chose will appear)

6. Q5-1. Specify the 'other' type of tool or technique used.

Name of tool	Specify the type of technology used
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	
(Tool from Q5 will be auto populated if Other (specify) was chosen)	

If using Age inference models at Q5.

7. Q6. For the age inference models listed in Q5, specify all the indicators that Valve Corporation used to assess the age of end users on Steam and Steam Chat. (multiple response)

	Choose all that apply
Operating system indicators	☐
App store indicators	☐
Cross platform indicators	☐
Language analysis	☐
Voice analysis	☐
Image classifiers	☐
Video classifiers	☐
Device identifiers	☐
IP address indicators	☐
Traffic indicators	☐
Financial indictors	☐

Behavioural indicators (list the behavioural indicators)	☐
Other (specify)	☐
Other (specify)	☐
Other (specify)	☐

If yes (a) at Q2

8. Q7. Specify when each of the tools and techniques listed in response to Q3 were used:

	At sign up	To access Steam Chat	To access certain games	When an account has been flagged for review by automated tools/human moderators	In response to a user report	When the service is accessed on a particular device (e.g. console, PC, mobile)	To gain access to parental controls	Other
Name of tool from Q3 will be auto populated)	☐	☐		☐	☐	☐	☐	☐
As above	☐	☐		☐	☐	☐	☐	☐
As above	☐	☐		☐	☐	☐	☐	☐
As above	☐	☐		☐	☐	☐	☐	☐
As above	☐	☐		☐	☐	☐	☐	☐

If other (specify) was chosen for any response at Q7

9. Q7-2. Specify when the 'other' tool or technique was used on Steam and Steam Chat.

Name of tool	Specify
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	
(Tool from Q7 will be auto populated if Other (specify) was chosen)	

If used a tool to assess the age of end-users (Yes at Q2)

10. Q8. During the report period, did Valve Corporation or a third-party provider of a tool or technique assess the effectiveness of these tools and techniques used on Steam and Steam Chat?

Name of tool/technology	Yes – Valve Corporation assessed	Yes – Third-party provider assessed	No
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○
(Tool from Q3 will be auto populated)	☐	☐	○

If yes at Q8 (assessed accuracy of the tools)

11. Q9. What metrics did Valve Corporation (or the third-party provider of a tool or technique) use to assess the effectiveness of each tool and technique? Include the specific metrics, and any relevant standards or certification schemes that Valve Corporation relied on to evaluate the effectiveness of a tool in your answer.

Name of tool/technology	Specify the effectiveness metric used for the assessment
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

12. Q10. What was the result of the assessment for effectiveness of each tool and technique?

Name of tool/technology	Specify details of the result
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

If yes at Q8 (assessed accuracy of the tools)

13. Q11. What action was taken as a result of the assessment for each tool and technique?

Name of tool/technology	Specify the action taken
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	
(Tool from Q8 will auto populate if Yes is chosen)	

14. Q12. During the report period, what action did Valve Corporation take after it became aware that the age information it held about an end-user may be incorrect.

	Choose all that apply

Banned account	☐
Suspended account	☐
Directed to undergo age assurance	☐
Strike against account	☐
Other (specify)	☐

IF yes at Q2

15. Q13. During the report period, specify how many end-users were found to be incorrectly age assured by the tools and techniques identified at Q3 to assess the age of end-users.

16. Q14. Provide any other relevant information or context in relation to your responses to questions 1 to 13, including:
    a. whether Valve Corporation undertook any research or development work during the report period in relation to age assurance
    b. whether responses to these questions are affected by whether an end-user uses Steam and Steam Chat on particular devices (e.g. on particular interfaces (e.g. browser, mobile or in app)

Section 2: Staffing / Moderation

Expectations 6(2), 6(2A), 11 and 12.

17. Q15. As at 31 March 2026, provide the number of staff employed by Valve Corporation for the below categories.

	Specify number employed
Engineers employed by Valve Corporation who spend at least 50% of their time on trust and safety	
Content moderators employed by Valve Corporation	
Content moderators contracted employed by Valve Corporation	
Trust and safety staff employed by Valve Corporation (other than engineers and content moderators)	

18. Q16. As at 31 March 2026, provide the number of moderators (contracted or employed by Valve Corporation) trained in the following unlawful or harmful material or activity:

	Specify number of moderators trained in each following unlawful or harmful material or activity
Grooming	
Other CSEA material and activity	
Sexual extortion	
Violence material and activity	

19. Q17. As at 31 March 2026, specify which of the below languages Valve Corporation's trust and safety staff operated in.

	Choose all that apply
English	☐
Mandarin	☐
Arabic	☐
Vietnamese	☐
Cantonese	☐
Punjabi	☐
Other languages	☐

If other (specify) was chosen for any response at Q17

20. Q18. What is the total number of the **other** languages that the Valve Corporation's contractor trust and safety staff operated in?

Number of other languages (excluding those listed at Q17)	

21. Q19. Provide any other relevant information or context in relation to your responses to questions 15 to Q18.

Section 3: User reporting

Expectations 14(1A).

23. Q20. During the report period, specify the number of **global** end-user reports of unlawful or harmful material or activity on Steam and Steam Chat which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Number of **global** end-user reports on Steam	Number of **global** end-user reports on Steam Chat
Grooming		
Sexual extortion		
Other CSEA material (excluding games) and activity		
Violence material (excluding games) and activity		
Cyber-bullying		
Material and activity covered by Valve Corporation’s online hate policies		

24. Q21. During the report period, specify the number of **Australian** end-user reports of unlawful or harmful material or activity on Steam and Steam Chat which were reviewed by human moderators, concerning each of the following unlawful or harmful material or activity.

	Number of **Australian** end-user reports on Steam	Number of **Australian** end-user reports on Steam Chat
Grooming		
Sexual extortion		
Other CSEA material (excluding games) and activity		
Violence material (excluding games) and activity		
Cyber-bullying		
Material and activity covered by Valve Corporation's online hate policies		

24. Q22. During the report period, specify the median time taken to reach an outcome after an end-user made a report, where reports were reviewed by human moderators. Provide responses for the median time concerning each of the following unlawful or harmful material or activity on Steam and Steam Chat.

This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review.

Provide a response in minutes

	Median time taken (minutes)
Grooming	
Sexual extortion	
Other CSEA material (excluding games) and activity	
Violence material (excluding games) and activity	
Cyber-bullying	
Material and activity covered by Valve Corporation's online hate policies	

25. Q23. During the report period, specify the median time taken to reach an outcome after automated tools flagged potential unlawful or harmful material or activity on Steam and Steam Chat, where flags were reviewed by human moderators. Specify for each of the following unlawful or harmful material or activity.

    This metric should be calculated from the time that a user report is made, to a content moderation outcome or decision by a human moderator, such as removing the content, banning the account, or deciding that no action should be taken. The metric should not include circumstances where actions are taken without human intervention e.g. when there is very high confidence of the relevant harm being committed and therefore no human review

	Median time taken
Grooming	
Sexual extortion	
Other CSEA material (excluding games) and activity	
Violence material (excluding games) and activity	
Cyber-bullying	
Material and activity covered by Valve Corporation's online hate policies	

26. Q24. During the report period, specify the proportion in percentage of unlawful or harmful material or activity that was detected proactively vs reported by users on Steam, concerning the following unlawful or harmful material or activity.

	Detected proactively (%)	Reported by end-users (%)
Grooming		
Sexual extortion		
Other CSEA material (excluding games) and activity		
Violence material (excluding games) and activity		
Cyber-bullying		
Material and activity covered by Valve Corporation's online hate policies		

27. Q24-1. During the report period, specify the proportion in percentage of unlawful or harmful material or activity that was detected proactively vs reported by users on Steam Chat, concerning the following unlawful or harmful material or activity.

	Detected proactively (%)	Reported by end-users (%)
Grooming		
Sexual extortion		
Other CSEA material (excluding games) and activity		
Violence material (excluding games) and activity		
Cyber-bullying		
Material and activity covered by Valve Corporation's online hate policies		

27. Q25. Explain how the answers to questions Q20 to Q24 were calculated and provide any other context.

	Specify how answers were calculated and provide any other context
Number of **Global** end-user reports	
Number of **Australian** end-user reports	
Median time taken to reach outcome from **Global** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from **Australian** end-user reports that were reviewed by human moderators	
Median time taken to reach outcome from automated tools that were reviewed by human moderators	
Percentage of unlawful or harmful material or activity detected proactively vs reported by users	

28. Q25-1. During the report period, specify the number of reports (either human reports or automated detection) that Valve Corporation received about games which may include Class 1 material made available via the Steam service.

Section 4: Action taken against end-users

Expectations 14(1A) and 14(2)

29. Q26. During the report period, what action did Valve Corporation take after an end-user breached the terms of service and/or community guidelines (or equivalent) in relation to the following unlawful or harmful material or activity.

	Sexual extortion	Grooming	Other CSEA material and activity	Violence material and activity	Cyberbullying	Conduct that breaches Valve Corporation's online hate policies
Banned account	☐	☐	☐	☐	☐	☐
Suspended account	☐	☐	☐	☐	☐	☐
Strike/Warning given to end-user	☐	☐	☐	☐	☐	☐
Removed harmful content created by user (e.g. user-generated content, messages)	☐	☐	☐	☐	☐	☐
Prevented user from creating certain content (e.g. marketplace items)	☐	☐	☐	☐	☐	☐
Other (specify)	☐		☐ ☐	☐	☐	☐

31. Q28. During the report period, specify the number of times Valve Corporation took the following actions where games made available via the Steam service were identified as capable of producing Class 1 content:

	Number of times action was taken
Game was permanently removed from the Steam service	
Game was reviewed and found not to be capable of producing Class 1 content	
Game was removed from the Steam service and reinstated when the breach was addressed	
Law enforcement notified	
Developer banned	
Developer suspended	
Other (Specify)	

32. Q29. Provide any other relevant information or context in relation to your responses to questions 26 to 28, including whether responses to these questions are affected by whether an end-user uses Steam and Steam Chat on particular interfaces (e.g. on browser, mobile or in app)

Section 5: Tools and Techniques

Expectations 6(2), 6(2A), 11 and 12.

33. Q30. During the report period, did Valve Corporation use tools and/or techniques on Steam and Steam Chat to detect the following unlawful or harmful material or activity?

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Other CSEA material and activity	o	o
Violence material and activity	o	o
Attempts to migrate children to another service	o	o

If used tool/techniques to identify harms (Yes for any at Q30)

34. Q31. Name all the tools and techniques used and which harm types they cover.

	Grooming [IF yes to Grooming at Q29]	Sexual extortion [IF yes to Sexual extortion at Q29]	Other CSEA material and activity [IF yes to Other CSEA at Q29]	Violence material and activity [IF yes to Violence at Q29]	Attempts to migrate children to another service [IF yes to attempts to migrate at Q29]
Tool 1 (Specify)	☐	☐	☐	☐	☐
Tool 2 (Specify)	☐	☐	☐	☐	☐
Tool 3 (Specify)	☐	☐	☐	☐	☐
Tool 4 (Specify)	☐	☐	☐	☐	☐
Tool 5 (Specify)	☐	☐	☐	☐	☐
Tool 6 (Specify)	☐	☐	☐	☐	☐
Tool 7 (Specify)	☐	☐	☐	☐	☐
Tool 8 (Specify)	☐	☐	☐	☐	☐
Tool 9 (Specify)	☐	☐	☐	☐	☐
Tool 10 (Specify)	☐	☐	☐	☐	☐

If used tool/techniques to identify violence material or violence activity at Q31

35. Q32. Specify the types of 'violence material and/or activity' the tool/technique is used to identify.

	Specify below

(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	
(Tool from Q31 will auto populate if Violence material and activity were chosen)	

If used tool/techniques to identify harms (Yes for any at Q30)

36. Q33. For each tool and technique identified at Q31, specify which part of the service it is used on.

[Steam response options]	Steam Discussions	Workshop Items	Reviews	Screenshots	Artwork	Broadcasts	Broadcast Chats	Videos	Game Titles	Other (specify)
[Steam Chat response options]	Steam Chat (Text chats)	Steam Chat (Community group chats)	Steam Chat (Voice chat)							
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐		☐

IF other at Q33

36. Q33-1. Specify the 'other' part of the service where the tool or technique was used.

	Specify
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	
(Tool from Q31 will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

36. Q34. For each tool and technique identified at Q31, specify the type of tool or technique.

	Language analysis tool (text) `	Language analysis tool (audio)	AI classifier	Hash-matching tool	Signals-based detection (e.g. behavioural indicators, financial indicators (specify)	Other (e.g. detecting URL join links) (specify)
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐
(Tool from Q31 will auto populate)	☐	☐	☐	☐	☐	☐

If Other (specify) chosen for any tool at Q34.

37. Q34-1. Specify the other type of tool or technique for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

If Signals-based detection (specify) chosen for any tool at Q34.

38. Q35. Specify the signals used for each tool.

Name of tool	Specify
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	
(Tool from Q34 will be auto populated if Other (specify) was chosen)	

39. Q36. For each tool or technique identified Q31, specify whether the tool detects material before or after it is published (i.e. as part of a pre-screening process).

	Before material is published	After material is published	Provide any relevant details
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	
(Tool from Q31 will auto populate)	☐	☐	

If used hash-matching tool at Q34

40. Q37. For each hash-matching tool identified at Q34, specify the names of the hash-matching source databases used.

Choose all that apply.

	GIFCT	IWF	NCMEC	Other (specify)
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	
(Hash-matching tool from Q34 will auto populate)	☐	☐	☐	

Q37-1. Please specify the 'other' hash-matching source database for the tools below.

	Other (specify)
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

41. Q38. For each hash-matching tool identified at Q34, specify the frequency at which Valve Corporation updated the hashes it scanned on Steam and Steam Chat against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (Specify)
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o
(Hash-matching tool from Q34 will auto populate)	o	o	o	o	o	o

41. Q38-1. Specify the 'other' frequency at which Valve Corporation updated the hashes it scanned on Steam and Steam Chat against these databases.

	Specify
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	
(Hash-matching tool from Q34 will auto populate)	

IF used language analysis tool at Q34

42. Q39. For each language analysis tool identified at Q34, specify all the languages it operated in.

Choose all that apply.

	English	Mandarin	Arabic	Vietnamese	Cantonese	Punjabi	Other	Language agnostic
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐

If other (specify) was chosen for any response at Q39

43. Q40. What is the total number of **other** languages that the language analysis tool operated in?

Number of other languages (excluding those listed at Q39)	

If use language analysis tool at Q34

44. Q41. For each language analysis tool identified at Q34, specify whether the tool has been trained to do any of the following:

	Key-word detection	Interpret sentence level context	Interpret conversation-level context	Distinguish joking/irony from serious intent	Interpret coded or indirect language (including use of emojis or symbols in words)	Interpret formatting or hashtags as context clues	Detect coercive or manipulative language	Detect attempts to migrate children to another service	Provide any other relevant details
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis	☐	☐	☐	☐	☐	☐	☐	☐	

tool from Q34 will auto populate)									
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	☐	☐	☐	☐	

If tool used language analysis tools at Q34

45. Q42. List all the organisations used to source keywords/training data for the language analysis tools listed below.

	GIFCT	IWF	NCMEC	Lantern	Other (specify)
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	
(Language analysis tool from Q34 will auto populate)	☐	☐	☐	☐	

IF other at Q42

45. Q42-1. Provide details on the other organisations used to source keyword/training data for the language analysis tools.

	Other (specify)
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	
(Language analysis tool from Q34 will auto populate)	

If tool used language analysis tools at Q34

46. Q43. For each language analysis tool identified at Q34, specify the frequency Valve Corporation updated the tool against these databases.

	Hourly/Multiple times a day	Daily	Weekly	Monthly	Annually	Other (specify)
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O
(Language analysis tool from Q34 will auto populate)	O	O	O	O	O	O

IF other at Q43

46. Q43-1. Provide details on the frequency that Valve Corporation updated the language analysis tools against the source keyword/training data.

47. ASK ALL who use tools Q33 yesQ44. During the report period, did Valve Corporation assess the accuracy of all the below tools used to detect the unlawful or harmful material or activity?

	Yes	No
(tool from Q31 will auto populate)	O	O

(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o
(tool from Q31 will auto populate)	o	o

If assessed accuracy of tools (Yes at Q44)

48. Q45. Provide details of the assessment methodology, specify details of any red teaming or simulated adversarial testing.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

49. Q46. What were the results of this assessment? Include **precision** and **recall rates** in your answer, and/or **any other metrics used to quantify the result**, with relevant context.

	Specify results
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If assessed accuracy of tools (Yes at Q44)

50. Q47. What action was taken as a result of the assessment for each tool?

	Specify action taken
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	
(Tool from Q44 that was assessed will auto populate)	

If used tool/techniques to identify harms (Yes for any at Q30)

51. Q48. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **Grooming**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Grooming at Q48.

57. Q48-1. If only in certain circumstances for Grooming, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	
(Tool from Q48 that are used in some circumstances will auto populate)	

53. Q49. For each tool and technique identified at Q31, specify whether it was used on all material by default or only in certain circumstances for **sexual extortion**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for sexual extortion at Q49

57. Q49-1. If only in certain circumstances for sexual extortion, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	
(Tool from Q49 that are used in some circumstances will auto populate)	

54. Q50. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **other CSEA material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for Other CSEA at Q50

57. Q50-1. If only in certain circumstances for other CSEA material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	
(Tool from Q50 that are used in some circumstances will auto populate)	

55. Q51. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances for **violence material and activity**?

	Used on all material by default	Used on material in some circumstances
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for violence material and activity at Q51

57. Q51-1. If only in certain circumstances for violence material and activity, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	

(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	
(Tool from Q51 that are used in some circumstances will auto populate)	

56. Q52. For each tool and technique identified at question 31, specify whether it was used on all material by default or only in certain circumstances **on attempts to migrate children to another service**?

	Used on all material by default	Used on material in some circumstance
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o
(Tools from Q31 will auto populate)	o	o

If used tools only in certain circumstances for attempts to migrate children at Q52

57. Q52-1. If only in certain circumstances on attempts to migrate children to another service, specify all those circumstances (e.g. only when an account had been flagged as suspicious, when an account was used on a particular device).

	Specify all circumstances
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	
(Tool from Q52 that are used in some circumstances will auto populate)	

58. Q55. During the report period, did Valve Corporation use any tools or other measures to detect trades of items on Community Market that may be linked to grooming and/or sexual extortion?

    1. Yes (specify details)
    2. No

59. Q56. Specify the details of the tools or other measures used to detect trades of items on Community Market that may be linked to grooming and/or sexual extortion.

60. Q57. Provide any other relevant information or context in relation to your responses to questions 39 to 46, including:
    a. whether Valve Corporation undertook any research or development work during the report period in relation to proactive detection of the harms listed in Q30
    b. whether responses to these questions are affected by whether an end-user uses Steam and Steam Chat on particular devices (e.g. on browser, mobile or in app)

Section 6: Recidivism

Expectations 14(1A).

61. Q58. During the report period, did Valve Corporation use the below indicators to identify recidivism after an end user had been banned or suspended for CSEA or violence material and activity.

	CSEA	Sexual extortion	Violence material and activity
Device identifiers	☐	☐	☐
Phone number	☐	☐	☐
Behavioural indicators	☐	☐	☐
Email address	☐	☐	☐
Geographical indicators	☐	☐	☐
Financial indicators	☐	☐	☐
Profile picture	☐	☐	☐
Username	☐	☐	☐
Name	☐	☐	☐
Date of birth	☐	☐	☐
Display name	☐	☐	☐
Other (specify)	☐	☐	☐
Other (specify)	☐	☐	☐

If used indicators to identify recidivism at Q58.

62. Q59. Were indicators used by default in all cases where an account has been banned or suspended for **CSEA material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

63. Q60. Were indicators used by default in all cases where an account has been banned or suspended for **sexual extortion**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances

[Indicators chosen at Q58 will auto populate in the rows below]	○	○

64. Q61. Were indicators used by default in all cases where an account has been banned or suspended for **violence material and activity**, or only in certain circumstances?

	Used on all material by default	Used on material in some circumstances
[Indicators chosen at Q58 will auto populate in the rows below]	○	○

If used indicators to identify recidivism at Q58.

65. Q62. What specific action did Valve Corporation take based on these indicators? If the action taken differed based on the specific indicators, specify all those differences, e.g. automatically blocked accounts with these indicators from being created; flagged the account for human review etc.

	Specify action taken
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	
(Auto populate indicators used at Q58)	

66. Q63. Provide any other relevant information or context in relation to your responses to questions 58 to 62 including:
    a. whether Valve Corporation undertook any research or development work during the report period in relation to prevention of recidivism on Steam and Steam Chat
    b. whether responses to these questions are affected by whether an end-user uses Steam and Steam Chat on particular devices (e.g. on particular interfaces (e.g. browser, mobile or in app)

Section 7: Moderation of user-generated content

Expectations 14(1A).

NA

Section 8: Information sharing initiatives

Expectations 10(1) and 14(1A).

70. Q66. During the report period, did Valve Corporation share information with the following services or initiatives (including bi-lateral arrangements with other providers) for the purpose of minimising grooming/sexual extortion and violence material and activity on its service?

	Choose all that apply
Lantern	☐
Tech Coalition	☐
Fair Play Alliance	☐
Tech Against Terrorism	☐
Discord	☐
Twitch	☐
Steam	☐
Other Initiatives/Services (specify)	☐

If a member of information sharing initiative (any at Q66)

71. Q67. Explain the steps taken as a result of sharing information with the below initiatives.

	Specify steps taken
(Auto populate sharing initiative chosen at Q669)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	
(Auto populate sharing initiative chosen at Q66)	

72. Q68. Provide any other relevant information or context in relation to your responses to questions 66 to 67, including whether Valve Corporation undertook any research or development work during the report period in relation to collaborating with civil society organisations or other service providers to prevent harm on Steam and Steam Chat

Section 9: Off-platform monitoring

Expectations 6(2), 6(2A), 11 and 12.

73. Q69. During the report period, did Valve Corporation use off-platform monitoring (monitoring of activity on other services either provided internally or by third-party services) to identify accounts or communities present on its service that are engaged in the below harms.

	Yes	No
Grooming	o	o
Sexual extortion	o	o
Violence activity	o	o

If used off-platform monitoring (Yes at Q69)

74. Q70. Provide details, specifying what this involved and what third party services were used.

	Specify details	Specify names of third parties used
Grooming		
Sexual extortion		
Violence activity		

75. Q71. Provide any other relevant information or context in relation to your responses to Q69 and Q70, including whether Valve Corporation undertook any research or development work during the report period in relation to monitoring of other services to identify accounts or communities engaged in the harms listed at Q69.

Section 10: Other

Expectations 6(2), 6(2A) and 11.

76. Q72. During the report period, did Valve Corporation provide any help services or support to users who were identified as potential victims of grooming and/or sexual extortion?
    a. Yes
    b. No

IF yes at Q53

77. Q73. Provide details on the help services or support Valve Corporation provided to users who were identified as potential victims of grooming and/or sexual extortion.

78. Q74. As at 31 March 2026, specify the proportion of under 18 accounts in Australia that have parental supervision enabled.

79. Q75. Explain how the answer to Q74 was calculated and provide any other context, including whether the use of parental controls on Steam and Steam Chat are affected by whether an end-user uses Steam and Steam Chat on particular devices (e.g. on browser, mobile or in app).

80. Q76. During the report period, did Valve Corporation have agreements in place with its third-party game providers to ensure games made available via the Steam service do not and/or cannot contain Class 1 material?
    a. Yes
    b. No

80. Q76-1. Provide details of the agreements in place with third-party game providers to ensure games made available via the Steam service do not and/or cannot contain Class 1 material?

81. Q77. During the report period, did Valve Corporation undertake any of the following measures when reviewing games to be released on the Steam service:

	Choose all that apply
Using hash-matching technologies on games to ensure that they do not contain CSAM or violence material	☐
Checking game titles against keyword lists associated with CSEA or violence material and activity	☐
Checking whether the game provider has had previous games removed from Steam for distributing Class 1 material	☐
Checking whether the game provider had any patches available off-platform which would allow the game to contain Class 1 material after purchase	☐
Other (specify)	☐

82. Q77-1. Provide any other relevant information or context in relation to your responses to questions 77, including whether Valve Corporation undertook any research or development work during the report period in relation to improving its pre-screening process.

Section 11: Final question

83. Q78. Outline any further steps Valve Corporation is taking to meet Expectations 6(2), 6(2A), 10(1), 11, 12, 14(1A) and 14(2).

    Do not replicate information provided in previous responses here. This is an opportunity for Valve Corporation to outline information about other types of safety measures.

7 April 2026

X Corp.

Submitted via X's Legal Requests Submission form: legalrequests.x.com

Our Reference: INV-2026-03407

Removal notice requiring you to remove class 1 material from your service

(Under section 109 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 109 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to ensure the removal of class 1 material, specified in **Attachment A**, from your service **within 24 hours** after being given the Notice.

Background

On 13 March 2026, the eSafety Commissioner became aware of material, which is provided on your service, specifically material that advocates terrorism and material depicting, expressing or otherwise dealing with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults and has been Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (the **Material**). The Material is further described in **Attachment A** to the Notice.

Basis for giving the Notice

I have formed the view that:

- the Material is, or has been, provided by you, a social media service within the meaning of section 13 of the Act;
- the Material is, or was, class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia; and
- the Material is not provided on an exempt service under section 109(1)(d) of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email **requests@esafety.gov.au** once you have removed the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 109 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.

Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $825,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to class 1 material. The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material on X.com. We request your cooperation to prevent the further dissemination of class 1 material.

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Attachments: Notice under section 109 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A DESIGNATED INTERNET SERVICE

Under section 109 of the *Online Safety Act 2021* (Cth)

To: **X Corp.**

Submitted via X's Legal Requests Submission form: legalrequests.x.com

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 109 of the Act and requires you to take all reasonable steps to ensure the removal of the class 1 material specified in **Attachment A.**

I give this notice to you on the basis that I am satisfied that:

A. the material is provided on your service, which is a social media service within the meaning of section 13 of the Act;
B. the material is, or was, class 1 material within the meaning of section 106(1)(a) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film; and
    ii. The material has been classified as Refused Classification (RC) by the Classification Board under the Classification (Publications, Films and Computer Game) Act 1995 (Cth) (Classification Act)
C. the Material can be accessed by end-users in Australia, and
D. the Material is not provided on an exempt service under section 109(1)(d) of the Act.

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 109 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 7 April 2026
Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

ATTACHMENT A – the Material for removal

First instance of material	
Service on which the material is provided:	
Location of material: **Our reference: INV-2026-03001**	s 7(2)
Description of material:	

Information sheet: Right of

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (https://www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at https://www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Email: enquiries@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request; and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues:

https://www.esafety.gov.au/about-us/contact-us

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

14 April 2026

Amarutu Technology Ltd

By email: s 47G(1)(a) **@koddos.com and** s 47G(1)(a) **@koddos.com**

Our Reference: INV-2026-02839, INV-2026-02852, INV-2025-10794, INV-2026-03251, INV-2026-02857 and INV-2026-02859.

Removal notice requiring you to cease hosting class 1 material on your service

(Under section 110 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 110 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 110 of the Act (**the Notice**). The Notice requires you to take all reasonable steps to cease hosting class 1 material **within 24 hours** after being given the Notice.

Background

On 5 December 2025 and 23 February 2026, the eSafety Commissioner became aware of six instances of class 1 material which is hosted on your service, specifically material depicting, expressing or otherwise dealing with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults and is likely to be Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (collectively, the **Material**). The Material is further described in **Attachment A** to the Notice.

The first two instances of material depict content that has been classified as RC by the Classification Board on 29 March 2019.

The third and fourth instances of material contain content that is substantially the same as material that has previously been classified as RC by the Classification Board on 29 March 2019.

The fifth and sixth instances of material contain content that is substantially the same as material that has previously been classified as RC by the Classification Board on 6 November 2024.

Basis for giving the Notice

I have formed the view that:

- the Material is or has been provided on a social media service within the meaning of section 13 of the Act;
- the Material is or was class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia;

- the Material is not provided on an exempt service under section 109(1)(d) of tge Act;
- the Material is not provided on an exempt service under section 110(1)(d) of the Act; and
- the Material is hosted by your service, which is a hosting service within the meaning of section 17 of the Act.

On this basis, I have decided to give you the Notice.

Required Action

Please email **requests@esafety.gov.au** once you have ceased hosting the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 110 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.
Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice also means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $825,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Review Rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to class 1 material. The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material on watchpeopledie.tv. We request your cooperation to prevent the further dissemination of class 1 material.

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

Attachments: Notice under section 110 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A HOSTING SERVICE

Under section 110 of the *Online Safety Act 2021* (Cth)

To: **Amarutu Technology Ltd**

By email: s 47G(1)(a) **@koddos.com and** s 47G(1)(a) **@koddos.com**

I am a delegate of the eSafety Commissioner for the purposes of section 110 of the *Online Safety Act 2021* (Cth) (t**he Act**).

This removal notice is given to you under section 110 of the Act and requires you to take all reasonable steps to cease hosting the class 1 material specified in **Attachment A** (the **Material**)**.**

I give this notice to you on the basis that I am satisfied that:

With respect to the first and second instances of the Material:

a) the material is provided on a social media service within the meaning of section 13 of the Act;
b) the material is, or was, class 1 material within the meaning of section 106(1)(a) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film; and
    ii. The film has been classified by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (**Classification Act**);
c) the material can be accessed by end-users in Australia, and
d) the Material is not provided on an exempt service under section 109(1)(d) of the Act;
e) the material is not provided on an exempt service under section 110(1)(d) of the Act.
f) the Material is hosted by your service, which is a hosting service within the meaning of section 17 of the Act.

With respect to the third and sixth (inclusive) instances of the Material:

a) the material is provided on a social media service within the meaning of section 13 of the Act;
b) the material is, or was, class 1 material within the meaning of section 106(1)(b) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film;
    ii. The film has not been classified by the Classification Board under the Classification Act; and
    iii. If the film were to be classified by the Classification Board under the Classification Act, the film would likely to be classified as RC;
c) the material can be accessed by end-users in Australia;
d) the Material is not provided on an exempt service under section 109(1)(d) of the Act;
e) the material is not provided on an exempt service under section 110(1)(d) of the Act.

f) The Material is hosted by your service, which is a hosting service within the meaning of section 17 of the Act.

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 110 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 14 April 2026

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

ATTACHMENT A – the Material

Service on which the material is provided:	**Watchpeopledie.tv**
First instance of material	
Location of material: **INV-2026-02839**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Second instance of material	
Location of material: **INV-2026-02852**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Third instance of material	
Location of material: INV-2025-10794	s 7(2)
Description of material:	s 7(2)

Fourth instance of material	
Location of material: **INV-2026-03251**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Fifth instance of material	
Location of material: **INV-2026-02857**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Sixth instance of material	
Location of material: INV-2026-02859	s 7(2)
Description of material:	s 7(2)

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

Email: enquiries@esafety.gov.au

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Australian Government | eSafetyCommissioner

17 April 2026

X Corp.

By online portal: https://legalrequests.x.com/

Our Reference: **ACA-2026-0776394**
NOT-2026-00370

Removal notice requiring you to remove cyber-abuse material targeted at an Australian adult from your service

(Under section 88 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 88 of the Act (**the Notice**). The Notice requires you to take all reasonable steps to ensure the removal of the cyber-abuse material targeted at an Australian adult from your service **within 24 hours** of being given the Notice. The cyber-abuse material targeted at an Australian adult is identified in the Notice.

s 22

A/g Manager (EL2), Cyber Abuse Team

Delegate of the eSafety Commissioner

Enclosed: *Notice under* section *88 of the Act*

Information Sheet

REMOVAL NOTICE TO REMOVE CYBER-ABUSE MATERIAL FROM YOUR SERVICE

Under section 88 of the *Online Safety Act 2021* (Cth)

To: **X Corp.**

By online portal: https://legalrequests.x.com/

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 88 of the Act and requires you to take all reasonable steps to ensure the removal of the material from your service specified at the URL link.

Background

On 22 February 2026, the eSafety Commissioner received a complaint under section 36 of the Act (**the Complaint**) about cyber-abuse material targeted at an Australian adult that is available on a service that you provide (**the Material**).

The adult cyber-abuse material targeted at an Australian adult

The Material is available at:

s 47E(d), s 47F

The decision to give you this removal notice

Taking into account all of the circumstances, I have reached the view that the Material is cyber-abuse material targeted at an Australian adult, as:

1) the Material is provided on a social media service within the meaning of section 13 of the Act;
2) an ordinary reasonable person would conclude that it is likely that the Material is intended to cause serious harm to the Complainant (an Australian adult) because:
   a) s 47E(d), s 47F
   b) s 47E(d), s 47F
3) s 47E(d), s 47F

s 47E(d), s 47F

I am satisfied that:

a) the Material is provided on a social media service;
b) the Material was the subject of a Complaint that was made to the provider of the service;
c) the Material was not removed from the service within 48 hours after the complaint was made, or within a longer period that was allowed by the eSafety Commissioner;
d) a Complaint has been made to the eSafety Commissioner under section 36 of the Act about the Material; and
e) the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act.

On this basis, I have decided to give you the Notice.

Required action

You are required to take all reasonable steps to ensure the removal of the Material from your service **within 24 hours** of being given this Notice, or within such longer period as I allow if I grant you an extension.

Please email requests@esafety.gov.au once you have taken all reasonable steps to ensure the removal of the Material in compliance with this Notice.

If you have any questions about the Notice or if you require an extension of time to comply, contact our office by email to requests@esafety.gov.au as soon as you receive this Notice.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 88 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action being taken against you, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Date: 17 April 2026

s 22

s 22

A/g Manager (EL2), Cyber Abuse Team
Delegate of the eSafety Commissioner

Australian Government | eSafetyCommissioner

22 April 2026

Our reference: BOSE-2026-01

Epic Games Entertainment International GmbH

c/o s 47F

By email: s 47G(1)(a) @epicgames.com

Dear s 47F

Variation to non-periodic reporting notice requiring Epic Games Entertainment International GmbH ('Epic Games') to prepare a report about the extent to which it has complied with the basic online safety expectations

On 1 April 2026, the eSafety Commissioner gave a non-periodic reporting notice to Epic Games under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

Enclosed is a notice to Epic Games which varies the Notice by extending the period for compliance to **16:00 Australian Eastern Standard Time (AEST) on 1 June 2026.**

As a variation, this notice does not constitute a new decision to give a notice under section 56(2) of the Act.

If you require additional time to comply, you may request this by sending an email to industryBOSE@esafety.gov.au.

Required action

The Notice, as varied, requires Epic Games to prepare a report, in the manner and form specified in the Notice, about the extent to which it complied with one or more specified applicable basic online safety expectations during the period specified in the Notice and give the report to the Commissioner by 16:00 AEST on 1 June 2026 (the **Due Date**).

In addition to the Qualtrics report form specified in Schedule B to the Notice, on 17 April 2026, Epic Games was provided an additional Qualtrics report form to enable it to include details for up to 20 tools and techniques in repose to question 31. The Notice requires Epic Games to name all the tools and techniques used and which harm types they cover.

Please refer to **Schedule A** to the Notice for the specified applicable basic online safety expectations to be reported on by Epic Games. The definitions of relevant terms can be found at **Schedule C** to the Notice.

Failure to comply with the Notice (as varied) may result in enforcement or compliance action being taken.

Failure to comply

You must comply with the requirement under the Notice (as varied) to the extent that you are capable of doing so.

Failure to comply with the Notice (as varied) is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 each day for a single contravention by a body corporate, or other action as determined by the eSafety Commissioner.

False or misleading information or documents

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Review of decision to give notice under section 56(2) of the Act

Unless otherwise notified, you are required to comply with the Notice (as varied) even if you have made an application for internal or external review.

Yours sincerely,



Julie Inman Grant
eSafety Commissioner
Enclosed: *Variation Notice dated 22 April 2026*

VARIATION TO NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Epic Games Entertainment International GmbH

Attention: s 47F

By email: s 47G(1)(a) @epicgames.com

This notice varies the non-periodic reporting notice that was given to Epic Games Entertainment International GmbH ('Epic Games') on 1 April 2026 under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

I vary the Notice to extend the date by which Epic Games is required to comply, by substituting the words:

"being no later than **17:00 Australian Eastern Standard Time (AEST) on 18 May 2026**"

with the words,

"being no later than **16:00 Australian Eastern Standard Time (AEST) on 1 June 2026**"

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 in respect of a body corporate for a single contravention.

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Julie Inman Grant

eSafety Commissioner

22 April 2026

Australian Government | eSafetyCommissioner

6 May 2026

Our reference: BOSE-2026-102

Mojang AB

c/o s 47F Digital Safety Unit, Microsoft

By email: s 47F @microsoft.com

Dear s 47F

Variation to non-periodic reporting notice requiring Mojang AB to prepare a report about the extent to which it has complied with the basic online safety expectations

On 1 April 2026, the eSafety Commissioner gave a non-periodic reporting notice to Mojang AB under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

Enclosed is a notice to Mojang AB which varies the Notice by extending the period for compliance to **16:00 Australian Eastern Standard Time (AEST) on 18 May 2026.**

As a variation, this notice does not constitute a new decision to give a notice under section 56(2) of the Act.

If you require additional time to comply, you may request this by sending an email to industryBOSE@esafety.gov.au.

Required action

The Notice, as varied, requires Mojang AB to prepare a report, in the manner and form specified in the Notice, about the extent to which it complied with one or more specified applicable basic online safety expectations during the period specified in the Notice and give the report to the Commissioner by 16:00 AEST on 18 May 2026 (the **Due Date**).

Please refer to **Schedule A** to the Notice for the specified applicable basic online safety expectations to be reported on by Mojang AB. The definitions of relevant terms can be found at **Schedule C** to the Notice.

Failure to comply with the Notice (as varied) may result in enforcement or compliance action being taken.

Failure to comply

You must comply with the requirement under the Notice (as varied) to the extent that you are capable of doing so.

Failure to comply with the Notice (as varied) is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 each day for a single contravention by a body corporate, or other action as determined by the eSafety Commissioner.

False or misleading information or documents

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Review of decision to give notice under section 56(2) of the Act

Unless otherwise notified, you are required to comply with the Notice (as varied) even if you have made an application for internal or external review.

Yours sincerely,



Julie Inman Grant

eSafety Commissioner

Enclosed: Variation Notice dated 6 May 2026

VARIATION TO NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Mojang AB

Attention: s 47F Digital Safety Unit, Microsoft

By email: s 47F @microsoft.com

This notice varies the non-periodic reporting notice that was given to Mojang AB on 1 April 2026 under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

I vary the Notice to extend the date by which Mojang AB is required to comply, by substituting the words:

"being no later than **17:00 Australian Eastern Standard Time (AEST) on 11 May 2026**"

with the words,

"being no later than **16:00 Australian Eastern Standard Time (AEST) on 18 May 2026**"

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 in respect of a body corporate for a single contravention.

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Julie Inman Grant

eSafety Commissioner

6 May 2026

Australian Government | eSafetyCommissioner

7 May 2026

Our reference: BOSE-2026-104

Valve Corporation

c/o s 47F Valve Corporation

By email: s 47F @valvesoftware.com; cc s 47F @valvesoftware.com

Dear s 47F

Variation to non-periodic reporting notice requiring Valve Corporation to prepare a report about the extent to which it has complied with the basic online safety expectations

On 1 April 2026, the eSafety Commissioner gave a non-periodic reporting notice to Valve Corporation under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

Enclosed is a notice to Valve Corporation which varies the Notice by extending the period for compliance to **16:00 Australian Eastern Standard Time (AEST) on 25 May 2026.**

As a variation, this notice does not constitute a new decision to give a notice under section 56(2) of the Act.

If you require additional time to comply, you may request this by sending an email to industryBOSE@esafety.gov.au.

Required action

The Notice, as varied, requires Valve Corporation to prepare a report, in the manner and form specified in the Notice, about the extent to which it complied with one or more specified applicable basic online safety expectations during the period specified in the Notice and give the report to the Commissioner by 16:00 AEST on **25 May 2026** (the **Due Date**).

Please refer to **Schedule A** to the Notice for the specified applicable basic online safety expectations to be reported on by Valve Corporation. The definitions of relevant terms can be found at **Schedule C** to the Notice.

Failure to comply with the Notice (as varied) may result in enforcement or compliance action being taken.

Failure to comply

You must comply with the requirement under the Notice (as varied) to the extent that you are capable of doing so.

Failure to comply with the Notice (as varied) is a contravention of section 57 of the Act and could result in the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 each day for a single contravention by a body corporate, or other action as determined by the eSafety Commissioner.

False or misleading information or documents

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.

Review of decision to give notice under section 56(2) of the Act

Unless otherwise notified, you are required to comply with the Notice (as varied) even if you have made an application for internal or external review.

Yours sincerely,



Julie Inman Grant
eSafety Commissioner
Enclosed: Variation Notice dated 7 May 2026

VARIATION TO NON-PERIODIC REPORTING NOTICE TO PREPARE A REPORT ABOUT THE EXTENT TO WHICH THE PROVIDER OF A RELEVANT ELECTRONIC SERVICE COMPLIED WITH BASIC ONLINE SAFETY EXPECTATIONS

Under section 56(2) of the *Online Safety Act 2021* (Cth)

To: Valve Corporation

Attention: s 47F Valve Corporation

By email: s 47F @valvesoftware.com; cc s 47F @valvesoftware.com

This notice varies the non-periodic reporting notice that was given to Valve Corporation on 1 April 2026 under section 56(2) of the *Online Safety Act 2021* (Cth) (**the Act**) (the **Notice**).

I vary the Notice to extend the date by which Valve Corporation is required to comply, by substituting the words:

"being no later than **17:00 Australian Eastern Standard Time (AEST) on 11 May 2026**"

with the words,

"being no later than **16:00 Australian Eastern Standard Time (AEST) on 25 May 2026**"

Section 57 of the Act provides that a person must comply with a notice to the extent that the person is capable of doing so. Failure to comply with a notice may result in enforcement action including the commencement of civil penalty proceedings for a civil penalty order of up to AUD $825,000 in respect of a body corporate for a single contravention.

It is a serious offence under the *Criminal Code 1995* (Cth) to give false or misleading information or produce false or misleading documents to the eSafety Commissioner or the Office of the eSafety Commissioner.



Julie Inman Grant

eSafety Commissioner

7 May 2026

18 May 2026

BitChute

By email: report@bitchute.com and legal@bitchute.com

Our Reference: INV-2026-04306 and INV-2026-04308

Removal notice requiring you to remove class 1 material from your service

(Under section 109 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 109 of the Act (**the Notice**). The Notice requires you to take all reasonable steps to ensure the removal of Class 1 material from your service **within 24 hours** after being given the Notice.

Background

On 21 April 2026, the eSafety Commissioner became aware of class 1 material, specifically material that advocates terrorism that I am satisfied is class 1 material which is provided on your service (**the Material**). I am satisfied it is class 1 material because it is a film that advocates terrorism and has been classified Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). The Material is further described in **Attachment A** to the Notice.

The decision to give you the Notice
I have formed the view that:

- the Material is or has been provided on a social media service within the meaning of section 13 of the Act;
- the Material is or was class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia;
- the Material is not provided on an exempt service under section 109(1)(d) of the Act;

On this basis, I have decided to give you the Notice.

Required Action

Please email **requests@esafety.gov.au** once you have removed the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

For the purposes of this Notice, the eSafety Commissioner will accept 'geo-blocking' of the Material in Australia as substantive compliance with the removal requirement of this Notice. Geo-blocking refers to the practice of restricting access to, or delivery of, online content based on the geographical location of an end-user's IP address.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 109 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.

Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice also means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $825,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review Rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to class 1 material. The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material on Bitchute.com. We request your cooperation to prevent the further dissemination of class 1 material.

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

Attachments: Notice under section 109 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A SOCIAL MEDIA SERVICE

Under section 109 of the *Online Safety Act 2021* (Cth)

To: BitChute

By email: report@bitchute.com and legal@bitchute.com

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (t**he Act**).

This removal notice is given to you under section 109 of the Act and requires you to take all reasonable steps to ensure the removal of the class 1 material specified in **Attachment A** (the **Material**)**.**

I give this notice to you on the basis that I am satisfied that:

a) the material is provided on a social media service within the meaning of section 13 of the Act;
b) the material is, or was, class 1 material within the meaning of section 106(1)(a) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film;
    ii. The film has been classified on 27 February 2025 as RC by the Classification Board under the Classification (Publications, Films and Computer Games) Act 1995;
c) the material can be accessed by end-users in Australia;
d) the Material is not provided on an exempt service under section 109(1)(d) of the Act;

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 109 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 18 May 2026

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

ATTACHMENT A – the Material

First Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2026-04306**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Second Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2026-04308**	s 7(2) [redacted]
Description of material:	s 7(2) [redacted]

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500, Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

Email: enquiries@esafety.gov.au

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

11 June 2026

X Corp

Submitted via X's Legal Requests Submission form: legalrequests.x.com

Our Reference: INV-2026-04655, INV-2026-04651

Removal notice requiring you to remove class 1 material from your service

(Under section 109 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 109 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to ensure the removal of class 1 material, specified in **Attachment A**, from your service **within 24 hours** after being given the Notice.

Please note that all references to a 'social media service' in this Notice are not intended to exhaustively or exclusively define your service under the Act.

Background

On 13 May 2026, eSafety became aware of class 1 material which is provided on your service, specifically material that depicts child sexual abuse and is likely to be classified as Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (the **Material**). The Material is further described in Attachment A to the Notice.

On 18 May 2026, eSafety sent a voluntary content notification via the legal request submissions portal to notify X about the material. No response was received, and, as at the date of the Notice the material remains available on your service.

Basis for giving the Notice

I have formed the view that:

- the Material is, or has been, provided by you, a social media service within the meaning of section 13 of the Act;
- the Material is, or was, class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia; and
- the Material is not provided on an exempt service under section 109(1)(d) of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email requests@esafety.gov.au once you have removed the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 109 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.

Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $825,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to child sexual abuse material (class 1 material). The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material onX. We request your cooperation to prevent the further dissemination of child sexual abuse material.

If a X user publishes a document, including a legal notice, containing URL hyperlinks to child sexual abuse material, they may be charged with criminal offences for the dissemination of child sexual abuse material under Australian federal or State law.

In addition, informing the end-user or any other third party may serve to undermine the eSafety Commissioner's regulatory functions.

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

Attachments: Notice under section 109 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A SOCIAL MEDIA SERVICE

Under section 109 of the *Online Safety Act 2021* (Cth)

To: **X Corp**

Submitted via X's Legal Requests Submission form: legalrequests.x.com

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (t**he Act**).

This removal notice is given to you under section 109 of the Act and requires you to take all reasonable steps to ensure the removal of the class 1 material specified in **Attachment A.**

I give this notice to you on the basis that I am satisfied that:

a) the Material is provided on your service, which is a social media service within the meaning of section 13 of the Act
b) the Material is, or was, class 1 material within the meaning of section 106(1)(b) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film; and
    ii. The material has not been classified as Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Game) Act 1995* (Cth) (**Classification Act**); and
    iii. If the film were to be classified by the Classification Board under the Classification Act – the film would be likely to be classified as RC.
c) the Material can be accessed by end-users in Australia, and
d) the Material is not provided on an exempt service under section 109(1)(d) of the Act.

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 109 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 11 June 2026

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

ATTACHMENT A

Service on which the material is provided:	X Corp
Location of material:	s 7(2)
Description of material:	

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at https://www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: sing the **Contact Us** form on the eSafety Commissioner's website

Email: enquiries@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request; and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues:

https://www.esafety.gov.au/about-us/contact-us

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

19 June 2026

X Corp.

Submitted via X's Legal Requests Submission form: legalrequests.x.com

Our Reference: INV-2026-05319

Removal notice requiring you to remove class 1 material from your service

(Under section 109 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 109 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to ensure the removal of class 1 material, specified in **Attachment A**, from your service **within 24 hours** after being given the Notice.

Please note that all references to a 'social media service' in this Notice are not intended to exhaustively or exclusively define your service under the Act.

Background

On 19 June 2026, the eSafety Commissioner became aware of material which is provided on your service. The material is class 1 material which is provided on your service, specifically material depicting, expressing or otherwise dealing with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults and is Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) (collectively, the **Material**). The Material is further described in **Attachment A** to the Notice.

On 6 November 2024, the Classification Board classified a video 25 seconds in length as Refused Classification **(RC)**, pursuant to item 1(a) of the films table of the National Classification Code (the **Code**).

The material contains content that is substantially similar to material that has previously been classified as RC by the Classification Board on 6 November 2024.

Basis for giving the Notice

I have formed the view that:

- the Material is, or has been, provided by you, a social media service within the meaning of section 13 of the Act;
- the Material is, or was, class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia; and
- the Material is not provided on an exempt service under section 109(1)(d) of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email **requests@esafety.gov.au** once you have removed the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 109 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) for a single contravention by a body corporate.

Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $825,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to class 1 material. The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material on X.com. We request your cooperation to prevent the further dissemination of class 1 material.

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Attachments: Notice under section 109 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A DESIGNATED INTERNET SERVICE

Under section 109 of the *Online Safety Act 2021* (Cth)

To: **X Corp.**

Submitted via X's Legal Requests Submission form: legalrequests.x.com

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 109 of the Act and requires you to take all reasonable steps to ensure the removal of the class 1 material specified in **Attachment A.**

I give this notice to you on the basis that I am satisfied that:

A. the material is provided on your service, which is a social media service within the meaning of section 13 of the Act;
B. the material is, or was, class 1 material within the meaning of section 106(1)(a) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film; and
    ii. The material has been classified as Refused Classification (RC) by the Classification Board under the Classification (Publications, Films and Computer Game) Act 1995 (Cth) (Classification Act)
C. the Material can be accessed by end-users in Australia, and
D. the Material is not provided on an exempt service under section 109(1)(d) of the Act.

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 109 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $825,000 (AUD) following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 19 June 2026
Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

ATTACHMENT A – the Material for removal

First instance of material	
Service on which the material is provided:	**X**
Location of material: **Our reference: INV-2026-05319**	s 7(2)
Description of material:	s 7(2)

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (https://www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at https://www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Email: foi@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request; and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues:

https://www.esafety.gov.au/about-us/contact-us

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Australian Government | eSafetyCommissioner

10 July 2026

X Corp.

865 FM 1209 Bldg. 2
Bastrop, TX 78602
United States of America

By online portal: **X's online legal request submission site (https://www.legalrequests.twitter.com/forms/landing_disclaimer)**

Our references: **NOT-2026-00509**
ACA-2026-H0Y2C5

Removal notice requiring you to remove cyber-abuse material targeted at an Australian adult from your service
(Under section 88 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (the ***Act***).

Please see enclosed a removal notice given to you under section 88 of the Act (the ***Notice***). The Notice requires you to take all reasonable steps to ensure the removal of the cyber-abuse material targeted at an Australian adult from your service **within 24 hours** of being given the Notice.

Please note that all references to a 'social media service' in this Notice are not intended to exhaustively or exclusively define your service under the Act.

s 47F, s 47E(c)
Executive manager (SES1), Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Enclosed: *Notice under* section *88 of the Act*

Schedule A

Information Sheet

REMOVAL NOTICE TO REMOVE CYBER-ABUSE MATERIAL FROM YOUR SERVICE
Under section 88 of the *Online Safety Act 2021* (Cth)

X Corp.

865 FM 1209 Bldg. 2
Bastrop, TX 78602
United States of America

By online portal: X's online legal request submission site (https://www.legalrequests.twitter.com/forms/landing_disclaimer)

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (the ***Act***).

This removal notice is given to you under section 88 of the Act and requires you to take all reasonable steps to ensure the removal of the material from your service specified in **Schedule A**.

Background

The eSafety Commissioner has received a complaint under section 36 of the Act (the ***Complaint***) about cyber-abuse material targeted at an Australian adult that is available on a service that you provide (the ***Material***).

The adult cyber-abuse material

The Material is available at: s 47F, s 47E(d)

The decision to give you this removal notice

Taking into account all of the circumstances, I have reached the view that the Material is cyber-abuse targeted at an Australian adult, as:

1. An ordinary reasonable person would conclude that it is likely that the Material was intended to have an effect of causing 'serious harm', as defined in section 5 of the Act, to a particular Australian adult based on the following:
    a. The Material was posted by an X user with the handle s 47F, s 47E(d) (the ***End User***).
    b. The Material is a reply to an earlier post by another end-user (the ***Parent Post***), which is critical of the targeted Australian adult s 47E(d), s 47F
    c. The Material references s 47E(d), s 47F

s 47E(d), s 47F

c. The Material s 47E(d), s 47F This is inherently capable of causing profound emotional distress to someone in the targeted Australian adult's position when published.
d. When considered together, the fact that the Material makes use of the s 47E(d), s 47F an ordinary reasonable person would likely consider that the Material was intended to have an effect of causing serious distress to the targeted Australian adult beyond 'mere ordinary emotional reactions such as those of only distress, grief, fear or anger'.

2. A person in the position of the targeted Australian adult would regard the material as harassing based on the following:
   a. The Material was posted s 47E(d), s 47F
   b. The reference to s 47E(d), s 47F
   c. The Material goes beyond reasonable criticism of the targeted Australian adult's public comments or opinions s 47E(d), s 47F
   d. Having regard to the timing of the post s 47E(d), s 47F I am satisfied that a reasonable person in the position of the targeted Australian adult would conclude that the material is harassing.

3. A person in the position of the targeted Australian adult would regard the material as offensive based on the following:
   a. s 47E(d), s 47F
   b. s 47E(d), s 47F

The material does not appear to have any literary, artistic or educational merit.I am satisfied that:

The material does not appear to be of a legal, medical or scientific character.

1. the Material is provided on X, and that X is a social media service within the meaning of section 13 of the Act;
2. the Material was the subject of a complaint that was made to the provider of the service;
3. the Material was not removed from the service within 48 hours after the complaint was made and no longer period has been allowed by the eSafety Commissioner;
4. a complaint has been made to the eSafety Commissioner under section 36 of the Act about the Material; and
5. the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email **requests@esafety.gov.au** once you have taken all reasonable steps to ensure the removal of the Material in compliance with the Notice. Failure to comply with the Notice may result in compliance or enforcement action being taken against you without further notice.

If you have any questions about the Notice or if you require a longer period of time to comply, contact our office by email to requests@esafety.gov.au as soon as you receive this Notice.

For the purposes of this Notice, the eSafety Commissioner will accept 'geo-blocking' of the Material in Australia as substantive compliance with the removal requirement of this Notice.

Geo-blocking refers to the practice of restricting access to, or delivery of, online content based on the geographical location of an end-user's IP address.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 88 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Date: 10 July 2026

s 47F, s 47E(c)

Executive manager (SES1), Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Schedule A – The Material for removal

URL:

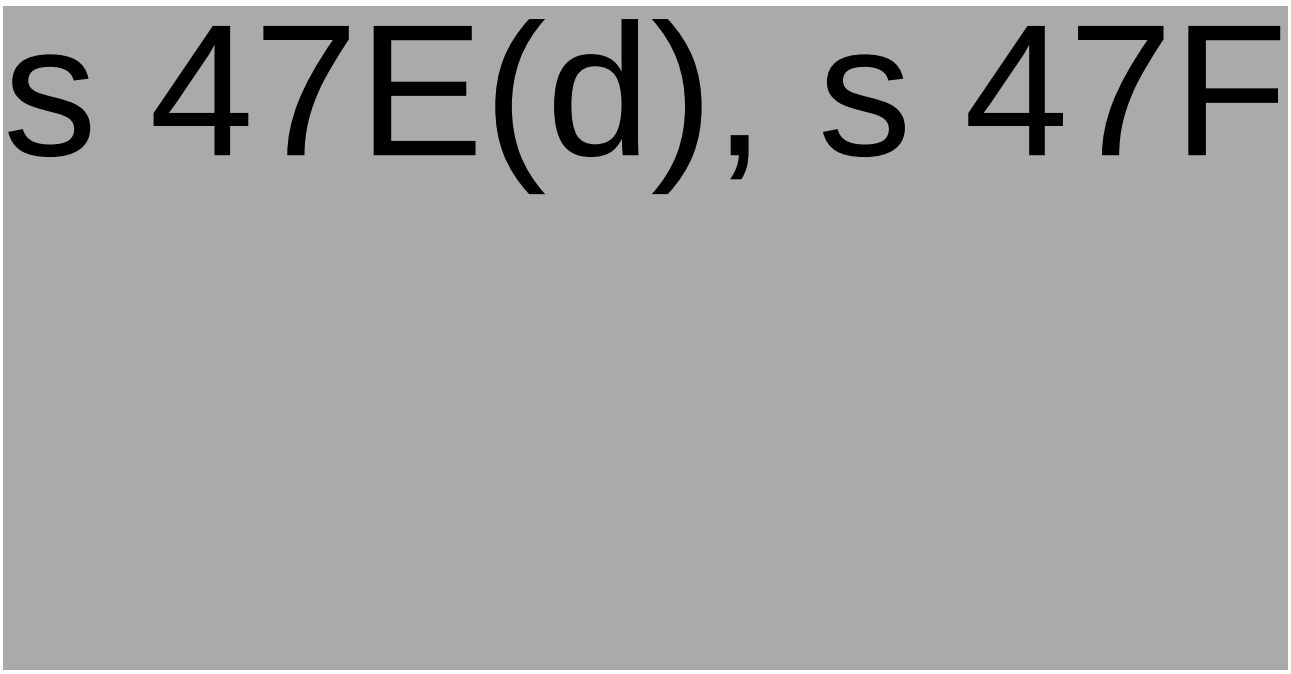
s 47F, s 47E(d)

Text:

s 47E(d), s 47F

Screenshot:

s 47E(d), s 47F



Screenshot of the Material, taken 3 July 2026

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us. **Requesting a statement of reasons for decision**

You may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

Email: foi@esafety.gov.au

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;

- provide information about each document to which you are seeking access to enable us to process your request, and

- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application: https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Australian Government | eSafetyCommissioner

15 July 2026

BitChute

By email: report@bitchute.com and legal@bitchute.com

Our Reference: INV-2025-06066, INV-2025-06067, INV-2025-06070, INV-2025-06071, INV-2025-06072, INV-2025-06074, INV-2026-05603 and INV-2026-05604.

Removal notice requiring you to remove class 1 material from your service

(Under section 109 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner (**eSafety**) for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 109 of the Act (**the Notice**). The Notice requires you to take all reasonable steps to ensure the removal of Class 1 material from your service **within 24 hours** after being given the Notice.

Background

On 8 October 2025, eSafety became aware of six pieces of material which is provided on your service, and on 9 July 2026, eSafety became aware of two pieces of additional material which is provided on your service. The material is class 1 material which is provided on your service, specifically material depicting, expressing or otherwise dealing with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults and is likely to be classified Refused Classification (**RC**) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). The Material is further described in **Attachment A** to the Notice.

The decision to give you the Notice
I have formed the view that:

- the Material is or has been provided on a social media service within the meaning of section 13 of the Act;
- the Material is or was class 1 material within the meaning of section 106 of the Act;
- the Material can be accessed by end-users in Australia;
- the Material is not provided on an exempt service under section 109(1)(d) of the Act.

On this basis, I have decided to give you the Notice.

Required Action

Please email **requests@esafety.gov.au** once you have removed the Material in compliance with the Notice.

If you have any questions about the Notice, or if you require a longer period of time to comply, contact our office by email to **requests@esafety.gov.au** as soon as you receive this Notice.

For the purposes of this Notice, the eSafety Commissioner will accept 'geo-blocking' of the Material in Australia as substantive compliance with the removal requirement of this Notice. Geo-blocking refers to the practice of restricting access to, or delivery of, online content based on the geographical location of an end-user's IP address.

Failure to comply

Under section 111 of the Act, you must comply with a requirement under a removal notice given under section 109 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Under section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), failure to comply with the Notice also means that you will commit a separate contravention of section 111 of the Act in respect of each day following the period specified for compliance with the Notice. This may attract additional penalties of up to $910,000 (AUD) each day for a single contravention by a body corporate following the end of the period specified for compliance with the Notice.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review Rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under eSafety's Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

Confidentiality of this Notice

This Notice contains URL hyperlinks to class 1 material. The Notice, its contents, and any investigation to which it relates should be kept confidential.

eSafety requests that the Notice not be shared with any third parties, including, but not limited to, the end-user/s responsible for posting the Material on Bitchute.com. We request your cooperation to prevent the further dissemination of class 1 material.

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

Attachments: Notice under section 109 of the Act
Information Sheet

REMOVAL NOTICE RELATING TO CLASS 1 MATERIAL GIVEN TO THE PROVIDER OF A SOCIAL MEDIA SERVICE

Under section 109 of the *Online Safety Act 2021* (Cth)

To: BitChute

By email: report@bitchute.com and legal@bitchute.com

I am a delegate of the eSafety Commissioner for the purposes of section 109 of the *Online Safety Act 2021* (Cth) (t**he Act**).

This removal notice is given to you under section 109 of the Act and requires you to take all reasonable steps to ensure the removal of the class 1 material specified in **Attachment A** (the **Material**)**.**

I give this notice to you on the basis that I am satisfied that:

a) the material is provided on a social media service within the meaning of section 13 of the Act;
b) the material is, or was, class 1 material within the meaning of section 106(1)(b) of the Act, as the following conditions are satisfied:
    i. The material is a film or the contents of a film;
    ii. The film has not been classified by the Classification Board under the Classification (Publications, Films and Computer Games) Act 1995;
    iii. If the film were to be classified by the Classification Board under the Act – the film would likely to be classified as RC;
c) the material can be accessed by end-users in Australia;
d) the Material is not provided on an exempt service under section 109(1)(d) of the Act;

You are required to comply **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 111 of the Act provides that a person must comply with a requirement under a removal notice given under section 109 of the Act to the extent the person is capable of doing so.

Failure to comply with a removal notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate following the end of the period specified for compliance with the Notice. A separate contravention occurs on each day where the material has not been removed within the required time period.

Date: 15 July 2026

Manager, Illegal and Restricted Content
Delegate of the eSafety Commissioner

ATTACHMENT A – the Material

First Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06066**	s 7(2)
Description of material:	S 7(2)

Second Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06067**	s 7(2)

Description of material:	s 7(2)

Third Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06070**	s 7(2)
Description of material:	s 7(2)

	s 7(2)

Fourth Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06071**	s 7(2)
Description of material:	s 7(2)

Fifth Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06072**	s 7(2)

Description of material:	s 7(2)

Sixth Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2025-06074**	s 7(2)
Description of material:	s 7(2)

	s 7(2)

Seventh Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2026-05603**	s 7(2)
Description of material:	s 7(2)

Eighth Instance of Material	
Service on which the material is provided:	**BitChute**
Location of material: **Our reference:** **INV-2026-05604**	s 7(2)

Description of material:	S 7(2)

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review, but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500, Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART for review in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

Email: enquiries@esafety.gov.au

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request, and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues.

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Australian Government | eSafetyCommissioner

31 July 2026

Aut O'Mattic A8C Ireland Ltd

ATTN: Chief Legal Officer

By Email Only: legal@wordpress.com

Our References: **ACA-2026-0791322**
ACA-2026-0822113

Removal notice requiring you to cease hosting cyber-abuse material targeted at an Australian adult
(Under section 90 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 90 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 90 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to cease hosting the material specified in the Notice **within 24 hours** of being given the Notice.

Background

On 11 April 2026, the eSafety Commissioner received a complaint under section 36 of the Act (the **Complaint**) about cyber-abuse material targeted at an Australian adult that is available on a service that you host (the **Material**).

eSafety's subsequent enquiries and investigation led to the assessment of the Material as cyber-abuse material targeted at an Australian adult. The Material is further specified in the Notice.

The decision to give you this removal notice

I have formed the view that:

a) the Material is provided on a designated internet service within the meaning of section 14 of the Act;
b) the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act;
c) the Material was the subject of a complaint that was made to the provider of the service;
d) the Material was not removed from the service within 48 hours after the complaint was made, or within a longer period that was allowed by the eSafety Commissioner;
e) a complaint has been made to the eSafety Commissioner under section 36(2) of the Act about the Material; and

f) you are the hosting service provider of the designated internet service that the Material is provided on.

On this basis, I have decided to give you the Notice.

Required action

You are required to take all reasonable steps to cease hosting the Material **within 24 hours** of being given this Notice, or within such longer period as I allow if I grant you an extension.

Please email requests@esafety.gov.au once you have taken all reasonable steps to ensure compliance with this Notice.

If you have any questions about the Notice or if you wish to request an extension of time to comply, contact our office by email to requests@esafety.gov.au. If you intend to request an extension, you should do so as soon as possible.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 90 of the Act to the extent you are capable of doing so.

Failure to comply with the Notice may result in enforcement action being taken against you, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

s 47F, s 47E(c)

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Enclosed: Notice under section 90 of the Act

Information Sheet

REMOVAL NOTICE TO CEASE HOSTING CYBER-ABUSE MATERIAL TARGETED AT AN AUSTRALIAN ADULT
Under section 90 of the *Online Safety Act 2021* (Cth)

To: Aut O'Mattic A8C Ireland Ltd

I am a delegate of the eSafety Commissioner for the purposes of section 90 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 90 of the Act and requires you to take all reasonable steps to cease hosting the material specified at the URL links below.

The cyber-abuse material targeted at an Australian adult (collectively, the Material)

The Material is available at the following URLs:

s 47F, s 47E(d)

I give this notice to you on the basis that I am satisfied that:

a) the Material is provided on the website s 47E(d), s 47F a designated internet service within the meaning of section 14 of the Act;
b) the Material is cyber-abuse material targeted at an Australian adult, for the following reasons:
    i. an ordinary reasonable person would conclude that it is likely that the Material was intended to cause serious harm to a particular Australian adult because:

        A. s 47E(d), s 47F

B. s 47E(d), s 47F [redacted]

ii. s 47E(d), s 47F [redacted]

c) the Material was the subject of a complaint that was made to the provider of the designated internet service;
d) the Material was not removed from the designated internet service within 48 hours after the complaint was made;
e) a complaint has been made to the eSafety Commissioner under section 36(2) of the Act about the Material; and
f) the Material is hosted by you, a hosting service provider.

You are required to comply with this requirement **within 24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension of time.

Section 91 of the Act provides that a person must comply with a requirement under a removal notice given under section 90 of the Act to the extent that the person is capable of doing so.

Failure to comply with the Notice may result in enforcement action being taken against you, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Date: 31 July 2026

s 47F, s 47E(c) [redacted]

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner

Information sheet: Right of Review

Internal review by the eSafety Commissioner or nominee

You have a right to seek an internal review of this decision under eSafety's Internal Review Scheme. An internal review is an impartial review of the merits of a decision. The purpose of an internal review is to consider whether the original decision made was the correct and preferrable one.

You must make an application for an internal review **within 30 days** of receiving the notice of this decision. If you intend to seek an internal review but are unable to make your application within 30 days, please email internalreview@eSafety.gov.au.

There are no fees associated with an application for internal review.

To request an internal review, you will need to download and complete the **Request for internal review form** available on eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

Please fill the form out and email it or post a hard copy to eSafety.

Email: internalreview@esafety.gov.au

Post: **Attention:** Internal Review
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

For additional information on eSafety's Internal Review Scheme, including the **eSafety Internal Review Procedure** and the **Online Safety (Internal Review Scheme) Instrument 2022**, please visit eSafety's website: www.esafety.gov.au/about-us/corporate-documents/internal-review.

External review by the Administrative Review Tribunal

You have a right to seek review of this decision by the Administrative Review Tribunal (**ART**). You can also request that the ART review a decision that has been made under the Internal Review Scheme.

It is recommended that you seek an internal review prior to seeking a review by the ART, however, there is no requirement to do so. You can choose to apply directly to the ART.

The ART is an independent body that can, among other things affirm, vary, or set aside the decision. If the ART sets aside the decision, it may make a substitute decision or remit the matter to the decision-maker to reconsider.

You must make any application for review to the ART in writing. The ART has a form available on its website which you can use.

Applications for review should be made **within 28 days** of being told about the decision.

You must enclose the application fee with your application. If you want to apply for the application fee to be reduced, you can obtain the application form for this from the ART.

The ART website (www.art.gov.au) has more information. If you have any questions about the ART's procedures and requirements, please contact the ART. Information about how to contact the ART is available at https://www.art.gov.au/contact-us.

Requesting a statement of reasons for decision

You may request a statement of reasons for this decision under section 268 of the *Administrative Review Tribunal Act 2024* (Cth). Your request needs to be made in writing **within 28 days** of being told of this decision. To request a statement of reasons, please email internalreview@esafety.gov.au.

Judicial Review

You may also be able to seek judicial review of this decision.

Judicial review does not consider the merits of the decision, and instead considers the legality of the decision, such as whether the decision-maker had power under the relevant statute to make the decision, followed the proper process and exercised the power in accordance with the law.

Should you wish to apply for judicial review of this decision, you may wish to obtain legal advice, as there may be costs involved.

Access to documents

You have a right to seek access to documents held by the eSafety Commissioner under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

You must apply to the eSafety Commissioner in writing through one of the following options:

Online: using the **Contact Us** form on the eSafety Commissioner's website

Email: foi@esafety.gov.au

Post: **Attention:** The FOI Coordinator
eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230

When you make your application, you should:

- state that the request is an application for the purpose of the FOI Act;
- provide information about each document to which you are seeking access to enable us to process your request; and
- provide a postal, email or fax address for us to reply to and which we can use to communicate with you about your application.

The eSafety Commissioner's website has more information on how to make an FOI application:

https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information

Complaints

If you are dissatisfied with the way that the eSafety Commissioner has handled this matter, we ask that you contact us using the **Contact Us** form on the eSafety Commissioner's website so that we can try to help resolve any issues:

https://www.esafety.gov.au/about-us/contact-us

If you are still dissatisfied, you may make a complaint to the Commonwealth Ombudsman. The Ombudsman usually prefers that your concerns are raised with the eSafety Commissioner first.

There is a Commonwealth Ombudsman office in each capital city. Further information may be obtained at www.ombudsman.gov.au.

Australian Government | eSafetyCommissioner

4 August 2026

Substack
s 47F

By email: s 47F **@substackinc.com**

Our Reference: **ACA-2026-Q4H2K2 / NOT-2026-00551**

Removal notice requiring you to remove cyber-abuse material targeted at an Australian adult from your service

(Under section 88 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 88 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to ensure the removal of the cyber-abuse material targeted at an Australian adult from your service **within 24 hours** of being given the Notice.

s 47F, s 47E(c)

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner
Date: 4 August 2026

Enclosed: Notice under section 88 of the Act
Information Sheet

REMOVAL NOTICE TO REMOVE CYBER-ABUSE MATERIAL FROM YOUR SERVICE

Under section 88 of the *Online Safety Act 2021* (Cth)

To: **Substack**

By email: s 47F **@substackinc.com**

Our Reference: **ACA-2026-Q4H2K2 / NOT-2026-00551**

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 88 of the Act and requires you to take all reasonable steps to ensure the removal of the material from your service specified in **Schedule A**.

Background

On 25 May 2026, the eSafety Commissioner received a complaint under section 36 of the Act (**the Complaint**) about cyber-abuse material targeted at an Australian adult that is available on a service that you provide (**the Material**).

This complaint was received following a direction by the Administrative Review Tribunal on 6 May 2026 that the Material is adult cyber-abuse targeted at an Australian adult for the purposes of section 7 of the Act.

The adult cyber-abuse material

The Material is available at:

s 47F, s 47E(d)

The decision to give you this removal notice

Taking into account all of the circumstances, I have reached the view that:

a) an ordinary reasonable person would conclude that it is likely that the Material is intended to cause serious harm to the Complainant s 47E(d), s 47F

b) an ordinary reasonable person in the position of the Complainant would regard the Material as being offensive s 47E(d), s 47F

s 47E(d), s 47F [redacted]

I am satisfied that:

a) the Material is provided on a designated internet service within the meaning of section 14 of the Act;
b) the Material was the subject of a complaint that was made to the provider of the service on 17 May 2026;
c) the Material was not removed from the service within 48 hours after the complaint was made, or within a longer period that was allowed by the eSafety Commissioner;
d) a complaint has been made to the eSafety Commissioner under section 36 of the Act about the Material; and
e) the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email requests@esafety.gov.au once you have taken all reasonable steps to ensure the removal of the Material in compliance with the Notice. Failure to comply with the Notice may result in compliance or enforcement action being taken against you without further notice.

If you have any questions about the Notice or if you require a longer period of time to comply, contact our office by email to requests@esafety.gov.au as soon as you receive this Notice.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 88 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

s 47F, s 47E(c)

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner
Date: 4 August 2026

Schedule A – The Material for removal

s 47E(d), s 47F

Australian Government | eSafetyCommissioner

4 August 2026

X Corp.

By online portal: X's online legal request submission site:

https://legalrequests.twitter.com/forms/landing_disclaimer

Our Reference: **ACA-2026-Q4H2K2 / NOT-2026-00550**

Removal notice requiring you to remove cyber-abuse material targeted at an Australian adult from your service

(Under section 88 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 88 of the Act (the **Notice**). The Notice requires you to take all reasonable steps to ensure the removal of the cyber-abuse material targeted at an Australian adult from your service **within 24 hours** of being given the Notice.

Please note that all references to a 'social media service' in this Notice are not intended to exhaustively or exclusively define your service under the Act.

s 47F, s 47E(c)

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner
Date: 4 August 2026

Enclosed: Notice under section 88 of the Act
Information Sheet

REMOVAL NOTICE TO REMOVE CYBER-ABUSE MATERIAL FROM YOUR SERVICE

Under section 88 of the *Online Safety Act 2021* (Cth)

To: **X Corp.**

By online portal: X's online legal request submission site:

https://legalrequests.twitter.com/forms/landing_disclaimer

Our Reference: **ACA-2026-Q4H2K2 / NOT-2026-00550**

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 88 of the Act and requires you to take all reasonable steps to ensure the removal of the material from your service specified in **Schedule A**.

Background

On 25 May 2026, the eSafety Commissioner received a complaint under section 36 of the Act (**the Complaint**) about cyber-abuse material targeted at an Australian adult that is available on a service that you provide (**the Material**).

This complaint was received following a direction by the Administrative Review Tribunal on 6 May 2026 that the Material is adult cyber-abuse targeted at an Australian adult for the purposes of section 7 of the Act.

The adult cyber-abuse material

The Material is available at:

s 47E(d), s 47F

The decision to give you this removal notice

Taking into account all of the circumstances, I have reached the view that:

a) an ordinary reasonable person would conclude that it is likely that the Material is intended to cause serious harm to the Complainant s 47E(d), s 47F

s 47E(d), s 47F

b) an ordinary reasonable person in the position of the Complainant would regard the Material as being offensive s 47E(d), s 47F

I am satisfied that:

a) the Material is provided on a social media service within the meaning of section 13 of the Act;
b) the Material was the subject of a complaint that was made to the provider of the service on 17 May 2026;
c) the Material was not removed from the service within 48 hours after the complaint was made, or within a longer period that was allowed by the eSafety Commissioner;
d) a complaint has been made to the eSafety Commissioner under section 36 of the Act about the Material; and
e) the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email requests@esafety.gov.au once you have taken all reasonable steps to ensure the removal of the Material in compliance with the Notice. Failure to comply with the Notice may result in compliance or enforcement action being taken against you without further notice.

If you have any questions about the Notice or if you require a longer period of time to comply, contact our office by email to requests@esafety.gov.au as soon as you receive this Notice.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 88 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of $910,000 (AUD) for a single contravention by a body corporate.

Giving false or misleading information or documents to eSafety is also an offence (see sections 137.1 and 137.2 of the Schedule to the *Criminal Code Act 1995* (Cth)).

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.

An external review is a review conducted by the Administrative Review Tribunal (**ART**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the ART has decided otherwise.

s 47F, s 47E(c)

Executive Manager, Complaints and Investigations Branch
Delegate of the eSafety Commissioner
Date: 4 August 2026

Schedule A – The Material for removal

s 47E(d), s 47F