Online Safety Act 2021

Compliance and Enforcement Policy

eSC CEP

October 2024

Australian Government | eSafetyCommissioner

Contents

About this policy

The eSafety Commissioner's **(eSafety's)** purpose and function is to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences.

This Compliance and Enforcement Policy **(Policy)** explains the compliance and enforcement powers available to eSafety under the *Online Safety Act 2021* (Cth) **(the Act)** and how eSafety will use these powers to promote online safety for Australians and protect Australians from online harms.

eSafety uses a range of tools to encourage compliance and prevent and respond to contraventions of the Act in line with our three pillars of purpose: prevention, protection and proactive change.[1]

This Policy explains eSafety's compliance and enforcement activities under the Act in relation to:

- administering a complaints scheme to investigate and remove cyberbullying material targeted at an Australian child **(child cyberbullying)**
- administering a complaints scheme to investigate and remove cyber abuse material targeted at an Australian adult **(adult cyber abuse)**
- administering a complaints and objections scheme to investigate and remove intimate images shared without the consent of the person depicted and to prevent the non-consensual sharing of intimate images **(image-based abuse)**
- administering the Online Content Scheme to investigate, restrict and/or remove the accessibility of illegal and restricted online content, including class 1 material[2] and class 2 material[3] accessible online from Australia **(illegal and restricted content)**
- preventing Australians from using the internet to access material that promotes, incites, instructs in, or depicts abhorrent violent conduct material **(abhorrent violent conduct)**
- directing compliance with applicable registered industry codes **(industry codes)** which set out minimum compliance measures that industry participants are required to take to protect Australians from class 1A material[4] and class 1B material[5], and enforcing compliance with such a Direction
- administering and enforcing reporting requirements by online service providers in accordance with the Basic Online Safety Expectations (**the Expectations**; also sometimes referred to as **the BOSE**).

eSafety registered six of the eight draft industry codes submitted by industry associations addressing class 1A material and class 1B material. In addition, eSafety has registered industry standards that will apply to the two further sections of the online industry identified in Part 9 of the Act, taking effect on 22 December 2024.

[1]Safety Strategy 2022-2025. [2]'Class 1 material' is defined in s 106 of the Act and include illegal material such as child abuse material, child sexual exploitation material and abhorrent violent material. [3]'Class 2 material' is defined in s 107 of the Act and include restricted material such as mainstream pornography and other material not suitable for audiences under 18 years. [4]'Class 1A material' is defined in the Head Terms to the Online Consolidated Industry Codes of Practice for the Online Industry (12 September 2023) (Head Terms) as a subcategory of class 1 material that includes child sexual exploitation material, pro-terror material, and extreme crime and violent material. [5]'Class 1B material' is defined in the Head Terms as a subcategory of class 1 material that includes crime and violence material and drug-related material.

The remainder of the sub-categories – class 1C material[6], class 2A material[7], class 2B material[8] – will be covered by a second phase of industry codes and/or standards.

Strategic context

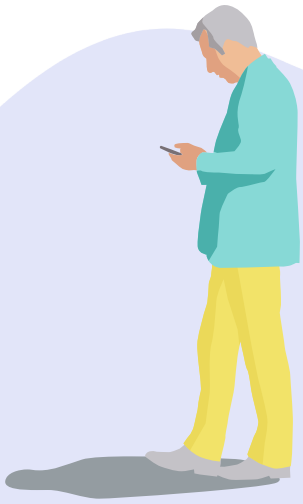
The statutory functions set out under section 27 of the Online Safety Act determine the key focus and activities of eSafety. The **eSafety Strategy 2022-2025** outlines how we will prioritise those activities to help Australians of all ages enjoy safer and more positive experiences online through until 2025.

Building on eSafety's experience administering the *Enhancing Online Safety Act 2015* and the *Online Safety Act 2021*, eSafety will continue to prevent and help remediate online harm and improve safety standards.

Based on evidence, research and data, eSafety will apply compliance and enforcement powers in a fair, transparent and proportionate way to limit the impact of harm to the user and to deter future wrongdoing by the platform or perpetrator. While eSafety may take graduated measures to act against online harm, there will be times when immediate and firm enforcement action is warranted due to the circumstances and severity of the harm.

eSafety will drive continuous improvements in the safety of online service providers by reviewing the effectiveness of their efforts to keep their users safe, and by providing practical recommendations and tools to support better outcomes.

eSafety's **Regulatory Posture and Regulatory Priorities document** will be updated periodically to inform stakeholders of the priorities of eSafety.



[6]Development of industry codes under the Online Safety Act Position Paper published by eSafety in September 2021 (Industry Codes Position Paper) identifies class 1C material as a subcategory of class 1 material that includes material that describes or depicts specific fetish practices or fantasies. [7]The Industry Codes Position Paper identifies class 2A material as a subcategory of class 2 material that includes material that depicts actual (not simulated) sex between consenting adults. [8]The Industry Codes Position Paper identifies class 2B material as a subcategory of class 2 material that includes material that includes realistically simulated sexual activity between adults and material which includes high impact nudity.

Outline of eSafety's compliance and enforcement powers

Table 1 sets out an overview of eSafety's statutory activities under the Act.

This document, and the steps described in it, should be read in conjunction with the specific regulatory guidance that eSafety has published for each scheme. Links to the relevant regulatory guidance are set out in the table.

The compliance and enforcement activities available to eSafety across its functions include the following.

1. Giving:
    - a removal notice
    - an end-user notice
    - a remedial direction
    - a service provider notification
    - a link deletion notice
    - an app removal notice
    - a blocking notice
    - a reporting notice or determination about compliance with the Expectations
    - a direction to comply with an industry code.
2. Where a civil penalty provision has been contravened:[9]
    - giving a formal warning
    - giving an infringement notice
    - accepting an enforceable undertaking
    - seeking a court-ordered injunction
    - seeking a court-ordered civil penalty
    - seeking another order in the Federal Court.

Not every option is available in relation to each statutory scheme.

eSafety will often also informally request that online service providers review and remove harmful online material and take appropriate action in accordance with their terms of service in the first instance. We have found that this generally results in faster removal of harmful online material, which is a better outcome for Australians targeted or affected by it.

This Policy also deals with circumstances where a civil penalty provision of the Act has been contravened and enforcement action may be appropriate.

Each of these statutory activities and powers is described in more detail in this Policy.

[9]The enforcement options available for each civil penalty provision of the Act are set out in **Attachment A**.

Table 1: Functions and powers under the Act where compliance and enforcement action may be taken (Part 1)

Child Cyberbullying Scheme	Image-Based Abuse Scheme	Adult Cyber Abuse Scheme	Online Content Scheme
Description of the statutory functions and powers			
Complaints scheme to address the cyberbullying of Australian children across a range of online services.	Complaints and objections scheme to address the sharing of, and threats to share, intimate images with or without the consent of the person depicted.	Complaints scheme to address online material targeted at Australian adults which is both intended to cause serious harm and is menacing, harassing or offensive.	Complaints scheme to address the availability of illegal and restricted online content (referred to in the Act as class 1 material and class 2 material) minimise children's exposure to age-inappropriate material online.
Who can make a complaint?			
An Australian child who has reason to believe they were or are the target of cyberbullying material.[10] A responsible person who has reason to believe that cyberbullying material was or is targeted at an Australian child and who is the child's parent or guardian or authorised by the child to make the complaint.[11] An 18 year old Australian who has reason to believe that, when they were a child, they were a target of cyberbullying material (so long as the complaint is made within a reasonable time and within 6 months after the person reached 18 years).[12]	A person depicted in an intimate image who has reason to believe s 75 of the Act[13] has been contravened.[14] A person authorised on behalf of the person depicted in the intimate image. This includes a parent or guardian of a child who has not reached 16 years of age and a parent or a guardian of a person who is incapable of managing their own affairs.[15]	An Australian adult who has reason to believe they were or are the target of adult cyber abuse material.[16] A responsible person who has reason to believe that adult cyber abuse material was or is targeted at an Australian adult and who has been authorised to make the complaint on behalf of the adult.[17]	A person who has reason to believe that Australians can access class 1 material and certain class 2 material through an online service provider.[18] A person who has reason to believe that Australians can access certain class 2[19] material through an online service provider and that access is not subject to a restricted access system.[20]

[10]s 30(1) of the Act. [11]s 30(2) of the Act. [12]s 30(1) of the Act. [13]Section 75 of the Act prohibits posting or threatening to post an intimate image without the consent of the person shown in the images. [14]s 32(1)-(2) of the Act. [15]s 30(3) of the Act. [16]s 36(1) of the Act. [17]s 36(2) of the Act. [18]s 38(1) of the Act. [19]Material that is or would likely be classified as R18+ or Category 1 restricted. [20]s 38(2) of the Act.

Child Cyberbullying Scheme	Image-Based Abuse Scheme	Adult Cyber Abuse Scheme	Online Content Scheme
Statutory options available to the eSafety Commissioner			
• Service provider notifications[21] • Removal notices[22] • End-user notices[23]	• Service provider notifications[24] • Removal notices[25] • Remedial directions[26]	• Service provider notifications[27] • Removal notices[28]	• Service provider notifications[29] • Removal notices[30] • Remedial notices[31] • Link deletion notices[32] • App removal notices[33]
Enforcement options in response to non-compliance with regulatory requirements			
See Attachment A			
Specific regulatory guidance			
Child Cyberbullying Scheme Regulatory Guidance – December 2023	Image-Based Abuse Scheme Regulatory Guidance – February 2024	Adult Cyber Abuse Scheme Regulatory Guidance – December 2023	Online Content Scheme Regulatory Guidance – December 2023

Table 1: Functions and powers under the Act where compliance and enforcement action may be taken (Part 2)

Abhorrent Violent Conduct Powers	Industry Codes	Industry Standards	Basic Online Safety Expectations
Description of the statutory functions and powers			
Powers to prevent the viral, rapid and widespread online distribution of material that promotes, depicts, incites or instructs in abhorrent violent conduct.	Registered industry codes which set out minimum compliance measures that relevant online industry participants commit to taking to protect Australians from class 1A and 1B material.	Determined industry standards which set out minimum compliance measures that relevant online industry participants must comply with to protect Australians from class 1A and 1B material.	The Australian Government's expectations of the steps to be taken by online service providers to keep Australians safe online (contained in a Statutory Determination). While compliance with the expectations is not mandatory, eSafety can require online service providers to provide information on the steps they are taking to comply with the expectations and publish statements on their compliance.

[21]s 73 of the Act. [22]ss 65 and 66 of the Act. [23]s 70 of the Act. [24]s 85 of the Act. [25]ss 77-79 of the Act. [26]s 83 of the Act. [27]s 93 of the Act. [28]ss 88-90 of the Act. [29]ss 113A, 118A and 123A of the Act. [30]ss 109, 110, 114 and 115 of the Act. [31]ss 119-120 of the Act. [32]s 124 of the Act. [33]s 128 of the Act.

Abhorrent Violent Conduct Powers	Industry Codes	Industry Standards	Basic Online Safety Expectations
Who can make a complaint?			
A person who has reason to believe that material that promotes, depicts, incites or instructs in abhorrent violent conduct is class 1 material or class 2 material. (The complaint can be made under the Online Content Scheme for illegal and restricted content.)	A person or body corporate in Australia who has reason to believe that an online industry participant has breached a registered industry code.	A person or body corporate in Australia who has reason to believe that an online industry participant has breached a determined industry standard.	N/A
Statutory options available to the eSafety Commissioner			
• Blocking request[34] • Blocking notice[35]	• Direction to comply with an industry code[36]	None	• Service provider notifications for non-compliance with a periodic or non-periodic reporting notice or determination, or non-compliance with the Expectations[37] • Periodic or non-periodic reporting notice or determination[38]
Enforcement options in response to non-compliance with regulatory requirements			
See Attachment A			
Specific regulatory guidance			
Abhorrent Violent Conduct Powers Regulatory Guidance – February 2024	Phase 1 Industry Codes (Class 1A and Class 1B Material) Regulatory Guidance – December 2023	Phase 2 Industry Standards (Class 1A and Class 1B Material) Regulatory Guidance (available late 2024)	Basic Online Safety Expectations Regulatory Guidance – December 2023

[34]s 95 of the Act. [35]s 99 of the Act. [36]s 143 of the Act. [37]ss 48, 55 and 62 of the Act. [38]ss 49, 52, 56 and 69 of the Act.

Considerations eSafety takes into account when determining approach to compliance and enforcement

eSafety will generally take a graduated and strategic approach to compliance and enforcement. In doing so, eSafety strives to balance the protection of Australians while ensuring an undue burden is not imposed on online service providers and end-users.

The action eSafety takes will always depend on the facts and the circumstances of each case. In determining whether to take compliance and enforcement action, and what action to take, eSafety may consider:

- the need to minimise the harm or risk of harm as quickly as possible
- the impact of the harmful online material or conduct on a person or the broader Australian community
- the extent to which any conduct represents a broader systemic issue
- the educative or deterrent effect of taking compliance or enforcement action
- repeated non-compliance by an online service provider, industry participant or end-user, and the likely risk of further non-compliance
- conduct that is of significant public interest or concern
- conduct that impacts eSafety's ability to effectively perform its statutory functions
- other factors that eSafety considers to be of relevance in the particular scenario.

Compliance activities

eSafety has a range of different compliance tools to encourage and direct online service providers and end-users to protect Australians from online harms.

Informal requests

eSafety will often approach online service providers informally to request that they review and take remedial action against harmful online material. Informal requests often lead to faster remedial action being taken compared to exercising compliance options under the Act.

These are examples:

- After receiving a complaint about child cyberbullying, adult cyber abuse, image-based abuse or illegal and restricted content, eSafety may approach the relevant online service provider in the first instance, asking it to review the material and take appropriate action in accordance with its own terms of service, if this is likely to result in quick removal of the harmful material.
- After identifying a breach of an industry code, eSafety may informally approach the industry participant to resolve the issue, instead of immediately giving the provider an enforceable direction to comply.

Voluntary tools under the Act

The Act also includes some mechanisms that are not enforceable.

For example, under the Abhorrent Violent Conduct Powers, eSafety may give a non-enforceable blocking request[39] to an internet service provider to take steps to disable access to the material. This is to give the provider the opportunity to take quick and voluntary action in the first instance. If such action is not taken, eSafety may then give the provider a blocking notice which is enforceable.

Further, under the *Online Safety (Basic Online Safety Expectations) Determination 2022* **(the Determination)**, the Minister for Communications has determined a set of basic online safety expectations for providers of social media services, relevant electronic services and designated internet services. Compliance with the Expectations is not mandatory. However, eSafety may issue notices to providers requiring them to report on their compliance with the Expectations. Compliance with these notices is mandatory. eSafety can also publish statements about whether providers have or have not complied with the Expectations.

Civil penalty provisions

The Act sets out civil penalty provisions for contraventions under the Act. The civil penalty provisions in the Act are listed in **Attachment A**. These include non-compliance with notices and directions given under the Act, requiring online service providers and/or end-users to take specific action.

Civil penalty provisions in the Act are enforceable and a contravention of a civil penalty provision may lead to eSafety taking enforcement action including civil penalties (see **Enforcement Action**).

Notices and directions which may attract enforcement action including civil penalties, if not complied with, are listed in Table 1. They include:

- **removal notices** requiring the provider of an online service to remove or take all reasonable steps to remove or stop hosting online material that meets the criteria for child cyberbullying, image-based abuse, adult cyber abuse or illegal and restricted content within 24 hours (or longer as directed)[40]
- **removal notices** requiring the end-user to take all reasonable steps to remove online material that meets the criteria for image-based abuse and adult cyber abuse within 24 hours (or longer as directed)[41]
- **end-user notices** requiring an end-user who is sharing cyberbullying material targeting a child to take specific steps including removing the material, refraining from sharing further cyberbullying material and apologising to the child[42]
- **remedial directions** requiring an end-user to take action to ensure that they do not share, or make a threat to share, image-based abuse material in the future[43]
- **remedial notices** requiring the provider of an online service to take steps to remove, stop hosting or restrict access to class 2 material within 24 hours (or longer as directed)[44]
- **link deletion notices** requiring a provider of an internet search engine service to stop providing a link to class 1 material within 24 hours (or longer as directed)[45]
- **app removal notices** requiring a provider of an app distribution service to stop enabling end-users in Australia to download from the service an app facilitating the sharing of class 1 material within 24 hours (or longer as directed)[46]

[39]s 95 of the Act. [40]ss 65, 66, 77, 79, 88, 90, 109, 110, 114, 115 of the Act. [41]ss 78 and 89 of the Act. [42]s 70 of the Act. [43]s 83 of the Act. [44]ss 119 and 120 of the Act. [45]s 124 of the Act. [46]s 128 of the Act.

- **blocking notices** requiring an internet service provider to take steps to disable access to abhorrent violent conduct material[47]
- **compliance directions** directing an industry participant to comply with a registered industry code[48]
- **periodic and non-periodic reporting notices and determinations** to compel a provider to give information about their compliance with the Basic Online Safety Expectations.[49]

In addition, there are a number of civil penalty provisions in the Act which don't require a notice or direction to be given. These include:

- **a general prohibition on image-based abuse**[50]
- **non-compliance with a registered industry standard** by a participant in that section of the online industry.[51]

eSafety may commence enforcement action where there has been non-compliance with these provisions.

Service provider notifications: child cyberbullying, adult cyber abuse, image-based abuse, or illegal and restricted content

The Act provides for different kinds of service provider notifications depending on the relevant functions under the Act.

This section explains when a service provider notification can be issued in response to child cyberbullying, adult cyber abuse, image-based abuse, or illegal and restricted content. For information about a service provider notification given for compliance or non-compliance with the Expectations, see **Service provider notifications: the Expectations**.

A service provider notification is a statement prepared by eSafety which is given to the provider of an online service. In this context, service provider notifications are intended to be used as a flexible compliance measure, to alert an online service provider to certain material available on their service and to encourage compliance.

There are two different service provider notifications which can be issued:

- A service provider notification may be given to an online service (with the consent of the complainant) to alert the service provider of material that is child cyberbullying, adult cyber abuse or image-based abuse on their service after receiving a complaint (or an objection notice).[52] This option is not available for illegal and restricted content.
- A service provider notification may be given to an online service provider if eSafety is satisfied that there were two or more occasions during the previous 12 months when child cyberbullying, adult cyber abuse, image-based abuse, or illegal and restricted content was available on a provider's service in breach of the service's terms of use. eSafety is also empowered to publish the statement on its website.[53] Publication of the statement may be used to encourage online service providers to comply with the Act to avoid negative publicity (sometimes referred to as 'name and shame' powers).

[47]s 99 of the Act. [48]s 143 of the Act. [49]ss 49 and 56 of the Act. [50]s 75 of the Act. [51]s 146 of the Act. [52]ss 73(1), 85(1), 93(1) of the Act. [53]ss 73(2), 85(2), 93(2), 113A, 118A, 123A of the Act.

The Act does not impose any time limits within which eSafety must issue a service provider notification.

A failure to take action after receiving a service provider notification does not attract any penalties or give rise to enforcement options. However, eSafety expects that an online service provider would take action and remove the harmful material without the need for eSafety to resort to other compliance action which may give rise to enforcement action.

eSafety will take into account an online service provider's response to a service provider notification when considering what other compliance or enforcement options to take in respect of the immediate circumstances. The response may also be taken into account in any future investigation in relation to material on that service.

Service provider notifications: the Expectations

A service provider notification may be issued by eSafety in connection with the Expectations in the following situations:

- eSafety may prepare and give to an online service provider a statement of non-compliance with a notice[54] or determination[55] requiring the provider to report on its compliance with one or more applicable expectations. This may be published on eSafety's website[56]
- eSafety may prepare and give to an online service provider a statement of non-compliance where eSafety is satisfied that the provider has contravened one or more of the Expectations for the provider's service. This may be published on eSafety's website[57]
- eSafety may prepare and give to an online service provider a statement that confirms its compliance with the Expectations for the provider's service at all times during a particular period, where eSafety is satisfied of this. This may be published on eSafety's website.[58]

A statement that confirms an online service provider's compliance with the Expectations provides positive reinforcement.

A statement of non-compliance introduces a reputational risk for a provider, creating a further incentive to comply with notices or determinations, or to comply with the Expectations, as relevant.

eSafety will have regard to the **Basic Online Safety Expectations Regulatory Guidance** in:

- assessing whether a provider is compliant with the expectations, or non-compliant with one or more applicable expectations
- deciding whether to give a service provider notification to a provider
- deciding whether to publish a service provider notification on eSafety's website
- taking other compliance or enforcement action in relation to the Expectations.

[54]ss 49 and 56 of the Act. [55]ss 52 and 59 of the Act. [56]ss 55 and 62 of the Act. [57]s 48(2) of the Act. [58]s 48(3) of the Act.

Referral of matter to law enforcement

There are a number of national and state/territory criminal offences that may apply to online harms. Victims of online harms should have the broadest range of remedies available to them. eSafety explains available options to complainants so they can make an informed choice about the most appropriate avenue for them in their circumstances. This may include recommending that a complainant report the matter to the relevant police force and providing instructions and tips on how to do so.

Victims of online harms can still make a complaint to eSafety, even if they have also reported the matter to police.

In some circumstances, eSafety must refer the matter to the relevant police force if satisfied that the material is of a sufficiently serious nature.[59]

General investigative powers

eSafety has discretion in how we conduct investigations. The Act provides eSafety with powers to require a person to meet with eSafety and to provide eSafety with information and documents in certain circumstances.

In addition to the exercise of its statutory powers, eSafety may also seek information on an informal basis from industry participants as part of its general compliance and investigatory functions.

Part 13 – Information-gathering powers: information about an end-user

eSafety can issue a written notice (section 194 Notice)[60] to an online service provider[61] requiring it to provide the contact details or other information about the identity of an end-user of the service, if eSafety believes that service has the information and the information is relevant to the operations of the Act.

eSafety can set the timeframe for complying with a section 194 Notice, as well as the manner and form in which the information should be provided.[62]

Penalties for failure to comply with the requirements of Part 13

A person who does not comply with a section 194 Notice to the extent they are capable of doing so is in breach of a civil penalty provision, with an applicable civil penalty of up to 100 penalty units for an individual.[63]

When determining whether it is appropriate to commence court proceedings to enforce a section 194 Notice, eSafety will consider, among other things:

- the significance of the non-compliance
- the extent to which non-compliance has undermined eSafety's functions and powers
- the extent to which the non-compliance has undermined any relevant investigation

[59]s 224 of the Act. [60]s 194(1) of the Act. [61]A provider of a social media service, a relevant electronic service or a designated internet service (s 194(1)(a) of the Act. [62]s 194(2) of the Act. [63]The maximum penalty that a court could order against a body corporate (which can include online service providers) can be five times more than the maximum penalty ordered against an individual.

- the impact of the non-compliance on the safety of the Australian public and/or specific complainant(s)
- any of the other relevant factors specified in the section of this document titled '**Considerations eSafety takes into account when determining compliance or enforcement action**'.

Part 14 – Investigative powers

eSafety has the power to, by written notice, require a person to:

- meet with eSafety to produce documents or to answer questions relevant to the subject matter of the investigation[64]
- provide documents or information to eSafety, relevant to the subject matter of an investigation[65]
- make available for inspection by eSafety any documents in the possession of the person that may contain information relevant to the subject matter of an investigation[66]
- and permit eSafety to make copies of any such documents.[67]

These powers can only be used for the purpose of an investigation about a child cyberbullying, adult cyber abuse or image-based abuse complaint, access to illegal and restricted content, and breach of a registered industry code or standard.[68]

Penalties for failure to comply with the requirements of Part 14

It is both a criminal offence and a breach of a civil penalty provision for a person who is required to answer a question, give evidence or produce documents under Part 14 to:[69]

- refuse or fail to take the oath or make the affirmation when required to do so
- refuse or fail to answer a question that the person is required to answer
- refuse or fail to produce a document that the person is required to produce.

The criminal offence carries a maximum penalty of 12 months imprisonment, while the civil penalty provision carries a maximum penalty of 100 penalty units.[70]

However, it is not an offence or a breach if:[71]

- the person can show that they have a reasonable excuse for the refusal or failure
- the answer to the question or the production of the document would tend to incriminate the person
- the person is a journalist and the answer to the question or the production of the document would tend to disclose the identity of a person who supplied information in confidence to the journalist.

When determining how to respond to a refusal to comply with a notice issued under Part 14, eSafety will consider, amongst other things:

- the significance of any refusal to comply
- the extent to which the refusal to comply has undermined eSafety's functions and powers

[64]s 199(a) of the Act. [65]s 199(b) of the Act. [66]s 203(a) of the Act. [67]s 203(b) of the Act. [68]s 198 of the Act. [69]s 205 of the Act. [70]ss 205(1)-(2) of the Act. Note the maximum penalty ordered against a corporation (which can include online service providers) can be five times more than the maximum penalty ordered against individual. [71]ss 205(3)-(5) of the Act.

- the extent to which the refusal to comply has undermined any relevant investigation
- the impact of the refusal on the safety of the Australian public and/or specific complainant(s)
- any other relevant factors in the section of this document titled '**Considerations eSafety takes into account when determining compliance or enforcement action**'.

Review rights

eSafety's decision to give an enforceable notice is subject to internal review by eSafety and to external merits review by the Administrative Review Tribunal.[72]

If eSafety refuses to give an enforceable notice following a valid complaint, this decision is also subject to internal review and to external merits review (this does not apply in relation to illegal and restricted content).[73]

Enforcement action

eSafety may take enforcement action where a civil penalty provision of the Act has been contravened including when enforceable notices are not complied with. The enforcement action may include:

- giving a formal warning
- giving an infringement notice
- accepting an enforceable undertaking
- seeking a court-ordered injunctions
- seeking court-ordered civil penalties
- seeking another order in the Federal Court

See **Attachment A** for a list of the civil penalty provisions under the Act and which enforcement options apply.

Formal warnings

What is a formal warning?

A formal warning notifies the recipient that they have breached a civil penalty provision or other provision of the Act but does not compel any action from them.[74]

A formal warning may be given to place an end-user or online service provider on notice where they have breached a civil penalty provision or otherwise failed to comply with certain provisions under the Act.[75] A formal warning may also be given for a breach of a provision of an industry code or standard registered under the Act.[76]

[72]ss 220, 220A of the Act. [73]ss 220, 220A of the Act. [74]See **Attachment A** for list of provisions which can give rise to a formal warning. [75]ss 51, 54, 58, 61, 68, 72, 76, 81, 84, 92, 112, 117, 122, 126, 130 of the Act. [76]ss 144, 147 of the Act.

Consistent with eSafety's graduated approach to enforcement, a formal warning may be appropriate where the non-compliance is relatively minor and where voluntary corrective action has been taken. eSafety may also rely on a formal warning when dealing with a breach of the Act by a minor, to provide education. Further, there may be instances under the schemes for child cyberbullying, adult cyber abuse and image-based abuse which involve more significant and serious conduct where it may still be appropriate to give a formal warning – for example, because the recipient of the warning is young, has other indicators of vulnerability, has indicated some form of remorse, or is assisting eSafety's investigation.

When can a formal warning be given?

eSafety may give a formal warning when an end-user or online service provider contravenes certain provisions of the Act as set out in **Attachment A**.

A formal warning may be used in conjunction with, or as an alternative to, other enforcement action. It is not a pre-condition to further enforcement action.

Will a formal warning be published?

eSafety may consider publishing a formal warning in appropriate circumstances to create a deterrent effect, and to ensure transparency regarding eSafety's regulatory decisions in line with the Act.[77] Publication of a formal warning will not disclose personal or sensitive information.

What are the consequences of not complying with a formal warning?

There are no penalties that can be imposed for inaction following the receipt of a formal warning.

eSafety may consider the fact that a warning has been given to a person (as well as the person's conduct following that warning) in deciding whether to take further enforcement action, particularly where additional contraventions are identified.

Enforceable undertakings

What is an enforceable undertaking?

An undertaking is a formal promise by a service provider or an individual to act, or refrain from acting, in a particular manner in order to prevent or respond to non-compliance. Once eSafety accepts an undertaking, it becomes enforceable by a court. Enforceable undertakings provide an opportunity for a person who has not complied with certain civil penalty provisions to be engaged in the resolution of the matter.

An enforceable undertaking can be a valuable tool to achieve a tailored, flexible and timely resolution of a matter.

When can an undertaking be accepted?

eSafety may accept an undertaking from an end-user or online service provider that has failed to comply with a civil penalty provision under the Act (see **Attachment A** for more detail).

An enforceable undertaking may be used in conjunction with, or as an alternative to, other enforcement action(s). For example, aspects of an undertaking could be directed to compliance

[77]Publication is made under sections 27 and 28 of the Act.

with a removal notice or remedial direction. An enforceable undertaking is not a pre-condition for further enforcement action.

While eSafety cannot require a person to offer an undertaking, eSafety may suggest that an enforceable undertaking is an appropriate option to resolve issues of concern and negotiate an undertaking that may be accepted. It may be beneficial when an end-user or online service provider is willing to engage with eSafety to rectify previous non-compliance and/or avoid future non-compliance.

What are the consequences of an enforceable undertaking?

If eSafety considers that a person has breached an enforceable undertaking, it may apply to a court for:

- an order directing the person to comply with the undertaking
- an order directing the person to pay to the Commonwealth an amount up to the amount of any financial benefit that the person has obtained directly or indirectly as a result of the breach
- any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach
- any other order that the court considers appropriate.[78]

Can an enforceable undertaking be varied or cancelled?

A person may withdraw or vary the undertaking at any time, but only with the written consent of eSafety.[79]

eSafety may, by written notice, cancel the undertaking.[80]

Injuctions

What is an injunction?

An injunction is a court order restraining a person from engaging in conduct, or requiring them to take certain steps, in relation to a contravention or proposed contravention of the Act.[81] eSafety can seek an injunction in the Federal Court of Australia or Federal Circuit Court of Australia.[82]

An injunction granted by the Court may:

- restrain a person who has contravened, is contravening or is proposing to contravene a relevant provision of the Act from engaging in that conduct[83]
- require a person who has contravened, is contravening or is proposing to contravene a relevant provision of the Act to take a specific action[84]
- require a person who has refused or failed, is refusing or failing, or is proposing to refuse or fail to take specific action to comply with a relevant provision of the Act, to take that action.[85]

[78]s 115 of the Regulatory Powers Act. [79]s 114(3) of the Regulatory Powers Act. [80]s 114(5) of the Regulatory Powers Act. [81]The sections which can be subject to an injunction under the Act are set out in s 165(1) of the Act. [82]s 165(3) of the Act. [83]s 121(1)(a) of the Regulatory Powers Act. [84]s 121(1)(b) of the Regulatory Powers Act. [85]s 121(2) of the Regulatory Powers Act.

When can eSafety apply for an injunction?

The provisions of the Act which can be subject to an injunction are set out in section 165(1) of the Act (see **Attachment A** for more detail). eSafety considers that an injunction will generally be appropriate where a person has caused or may cause significant harm and the matter is urgent, or other options to resolve a breach of the Act have been ineffective.

What are the consequences of an injunction?

If a person breaches an injunction they may be held in contempt of court, which is punishable by fines and/or imprisonment.

Can an injunction be discharged or varied?

The court may discharge or vary an injunction.[86]

Infringement notices

What is an infringement notice?

An infringement notice sets out the particulars of an alleged contravention of the Act and specifies a penalty that can be paid in lieu of further enforcement action being taken by eSafety.

If an infringement notice is paid, eSafety cannot pursue proceedings seeking a civil penalty order or an injunction for that specific contravention of the Act.[87] However, such proceedings may follow if an infringement notice is not paid.

Payment of an infringement notice is not an admission of liability.[88]

Who can give an infringement notice?

An infringement officer is empowered to issue an infringement notice.[89] Under the Act, an infringement officer is a member of the staff of the Australian Communications and Media Authority who is authorised, in writing, by the eSafety Commissioner to give an infringement notice.[90]

When can an infringement notice be given?

An infringement officer can issue an infringement notice if the officer believes on reasonable grounds that a person has contravened a provision set out in section 163(1) of the Act (see **Attachment A** for more detail).[91] eSafety considers that, generally, an infringement notice will be best suited for matters where eSafety determines that:

- the infringement notice will allow for a timely and efficient response to non-compliance without the need to bring court action and/or
- a financial penalty may deter future non-compliance with the Act.

Alternative options may be preferable where there is reason to believe that an infringement notice may not deter the person from engaging in similar behaviour in the future or the notice may cause or exacerbate financial hardship. Further, in most instances, it will not be appropriate to issue an infringement notice against a child or young person.

[86]s 123 of the Regulatory Powers Act. [87]s 107(d) of the Regulatory Powers Act. [88]s 107(e) of the Regulatory Powers Act. [89]s 101 of the Regulatory Powers Act. [90]s 163(2) of the Act. [91]s 103(1) of the Regulatory Powers Act.

An infringement notice must be given within 12 months after the day on which the contravention of the Act is alleged to have taken place.[92]

Amount payable under an infringement notice

Section 104 of the Regulatory Powers Act sets out the amount payable under an infringement notice.

If the notice relates to one alleged contravention under the Act, the penalty amount will be:[93]

- if the person is an individual – 12 penalty units
- if the person is a body corporate – 60 penalty units.

If the notice relates to more than one alleged contravention, the penalty amount will be multiplied by the number of alleged contraventions.[94] Where the contravention is a failure to do an act or thing within a specified period or before a particular time, a separate contravention occurs on each day until the act or thing is done.[95]

For any contravention, one penalty unit amounts to $330, effective late 2024.[96] This means that a recipient of an infringement notice would be required to pay:

- if the person is an individual – $3,960 for every alleged contravention
- if the person is a body corporate – $19,800 for every alleged contravention.

What are the consequences of an infringement notice?

If the recipient of the infringement notice pays the specified amount within 28 days, their liability is discharged. Court proceedings seeking a civil penalty order or an injunction may not be brought in relation to the alleged contravention.[97]

At any point before the end of those 28 days, the recipient can apply to eSafety or a delegate for an extension of time in which to pay the infringement notice. eSafety or a delegate may, at their discretion, extend that period. More than one extension may be given.[98]

If the infringement notice is not paid, eSafety may commence civil penalty or injunction proceedings (see next section on **Civil penalty orders**).

Can the recipient of an infringement notice seek to have it withdrawn?

Yes. The recipient of an infringement notice can write to eSafety to seek to have the notice withdrawn.[99] eSafety may also withdraw an infringement notice of their own volition.[100]

When deciding whether or not to withdraw an infringement notice, eSafety:[101]

- must take into account any written representations from the recipient seeking the withdrawal

[92]s 103(2) of the Regulatory Powers Act. [93]s 104(2) of the Regulatory Powers Act. This section requires that the amount payable in the infringement notice is the lesser of (a) one-fifth of the maximum penalty that a court could impose on the person for that contravention, and (b) 12 penalty units for an individual or 60 penalty units for a body corporate. Given the civil penalty attached to the provisions in relation to which an infringement notice may be issued is either for 100 or 500 penalty units, the lesser of those two options will always be the latter option. [94]s 104(3) of the Regulatory Powers Act. [95]s 93 Regulatory Powers Act. [96]The relevant penalty unit value will be that applicable at the time of the contravention at issue, as set out in the Crimes Act 1914 s 4AA. [97]s 107(1) of the Regulatory Powers Act. [98]s 105 of the Regulatory Powers Act. [99]s 106(1) of the Regulatory Powers Act. [100]s 106(2) of the Regulatory Powers Act. [101]s 106(3) of the Regulatory Powers Act.

- may take into account
  - whether a court has previously imposed a penalty on the person for a contravention of a provision of the Act subject to an infringement notice
  - the circumstances of the alleged contravention
  - whether the person has paid an amount, stated in an earlier infringement notice, for substantially similar conduct
  - any other matter considered relevant.

If a notice is withdrawn, eSafety may still commence civil proceedings against the person in relation to the alleged contravention(s).[102]

eSafety may publish information concerning the giving and payment of an infringement notice. eSafety will not publish information identifying a recipient of an infringement notice where the recipient is an individual.

eSafety will consider if publication is appropriate on a case-by-case basis. eSafety will consider, among other things, whether there is a strong public interest in publishing information about what enforcement action has been taken in response to a contravention of the Act, and the deterrent effect of publishing the infringement notice.

Civil penalty orders

What is a civil penalty order?

A civil penalty order is a court order requiring a person who is found to have contravened a civil penalty provision of the Act to pay the Australian Government a penalty.

A civil penalty order is the most serious enforcement option available to eSafety. Generally, a civil penalty order will be sought by eSafety in cases where the person has caused significant harm or engaged in multiple contraventions, or if other compliance and enforcement options have been ineffective.

Before seeking a civil penalty order against an end-user, eSafety may consider the particular person's circumstances, including any vulnerabilities or disadvantages.

When can eSafety apply for a civil penalty order?

eSafety can commence court proceedings seeking a civil penalty order against an end-user or online service provider who has contravened a civil penalty provision in the Act (see **Attachment A** for more details).

eSafety may apply for a civil penalty order in relation to the most serious contraventions of the Act or if other enforcement actions have been unsuccessful. eSafety may apply for a civil penalty order in conjunction with other court orders (such as an injunction) or concurrently with other actions under the Act.

eSafety must apply for a civil penalty order within 6 years of the alleged contravention.[103]

[102] s 104(1)(m) of the Regulatory Powers Act. [103] s 82(2) of the Regulatory Powers Act.

What are the consequences of a civil penalty order?

If the Court is satisfied that the person has contravened a civil penalty provision(s), it may order the person to pay the Australian Government a financial penalty the Court determines is appropriate.

The maximum civil penalty applicable to an individual is specified in each civil penalty provision in the Act. The maximum civil penalty applicable to a body corporate is five times the amount specified in the provision.[104]

Most provisions specify a maximum penalty of 500 penalty units for individuals. The maximum penalty ordered against a body corporate (including an online service provider) can be five times more than the maximum penalty ordered against an individual.

The only two provisions which have a lower civil penalty of 100 penalty units (for individuals) are those relating to non-compliance with eSafety's investigative and evidence-gathering powers.[105]

Where the contravention is a failure to do an act or thing within a specified period or before a particular time, a separate contravention occurs on each day until the act or thing is done.[106]

The following table shows the maximum penalty amounts per contravention, effective late 2024.[107]

Who?	Maximum penalty amount where the provision specifies 100 penalty units	Maximum penalty amount where the provision specifies 500 penalty units
Individual	$33,000	$165,000
Body corporate (up to 5 x maximum penalty)	$165,000	$825,000

Can a civil penalty order be appealed?

Yes. A civil penalty can be appealed through the court system.

Federal Court orders

Under the Act, if there have been at least two or more instances of non-compliance with an enforceable notice that has been issued for class 1 material or class 2 material during the previous 12 months (including in relation to a breach of a registered industry code or industry standard), eSafety may apply to the Federal Court for an order that, as the case requires, a person stop either:

- providing a social media service
- providing a relevant electronic service
- providing a designated internet service or
- supplying and internet carriage service.

eSafety can only apply for a Federal Court order if the continued operation of the service would represent a significant community safety risk.[108]

This is a significant power that is intended to be used as a last resort where other compliance and enforcement avenues for redress have failed.

[104]s 82(5) of the Regulatory Powers Act. [105]ss 195, 205(2) of the Act and the maximum penalty ordered against a body corporate (which can include online service providers) can be five times more than the maximum penalty ordered against individual. [106]S 93 Regulatory Powers Act. [107]The relevant penalty unit value will be that applicable at the time of the contravention at issue, as set out in the Crimes Act 1914 s 4AA. [108]ss 156–159 of the Act.

Attachment A: Enforcement options available to eSafety under the Act

Section	Provision	Maximum civil penalty[109]	Formal warning	Infringement notices	Enforceable undertakings	Injunctions
Part 4 – Basic Online Safety Expectations						
50	Non-compliance with a periodic reporting notice	500 penalty units	Section 51: For contravention of s 50	✓	✓	✓
53	Non-compliance with a periodic reporting determination	500 penalty units	Section 54: For contravention of s 53	✓	✓	✓
57	Non-compliance with a non-periodic reporting notice	500 penalty units	Section 58: For contravention of s 57	✓	✓	✓
60	Non-compliance with a non-periodic reporting determination	500 penalty units	Section 61: For contravention of s 60	✓	✓	✓
Part 5 – Child Cyberbullying Scheme						
67	Non-compliance with a removal notice	500 penalty units	Section 68: For contravention of s 67	✓	✓	✓
71	Non-compliance with an end-user notice	N/A	Section 72: For contravention of s 71	✗	✗	✓
Part 6 – Image-Based Abuse Scheme						
75	Sharing/threatening to share an intimate image	500 penalty units	Section 76: For contravention of s 75	✓	✓	✓
80	Non-compliance with a removal notice	500 penalty units	Section 81: For contravention of s 80	✓	✓	✓
83	Non-compliance with remedial direction (person sharing or threatening to)	500 penalty units	Section 84: For contravention of s 83	✓	✓	✓
Part 7 – Adult Cyber Abuse Scheme						
91	Non-compliance with a removal notice	500 penalty units	Section 92: For contravention of s 91	✓	✓	✓
Part 8 – Abhorrent Violent Conduct Powers						
103	Non-compliance with a blocking notice	500 penalty units	✗	✗	✓	✓

[109]The maximum civil penalty applicable to a body corporate is five times the amount specified in the provision, see s82(5) of the Regulatory Powers Act.

Section	Provision	Maximum civil penalty[109]	Formal warning	Infringement notices	Enforceable undertakings	Injunctions
Part 9 – Online Content Scheme						
111	Non-compliance with a Class 1 removal notice	500 penalty units	Section 112: For contravention of s 111	✓	✓	✓
116	Non-compliance with a Class 2 removal notice	500 penalty units	Section 117: For contravention of s 116	✓	✓	✓
121	Non-compliance with a Class 2 remedial notice	500 penalty units	Section 122: For contravention of s 121	✓	✓	✓
125	Non-compliance with a link deletion notice	500 penalty units	Section 126: For contravention of s 125	✓	✓	✓
129	Non-compliance with an app removal notice	500 penalty units	Section 130: For contravention of s 129	✓	✓	✓
143	Non-compliance with a direction to comply with an industry code	500 penalty units	Section 144: For contravention of s 143	✓	✓	✓
146	Non-compliance with an industry standard	500 penalty units	Section 147: For contravention of s 146	✓	✓	✓
153	Non-compliance with a service provider rule	500 penalty units	Section 155	✗	✗	✗
154	Contravention of a direction to not breach a service provider rule	500 penalty units	✗	✗	✗	✗
Part 13 – Information-gathering powers						
195	Non-compliance with a requirement to provide end-user identity information or contact details	100 penalty units	✗	✗	✗	✓
Part 14 – Investigative powers						
205	Non-compliance with a requirement to give evidence	100 penalty units (also has criminal penalty of imprisonment for up to 12 months)	✗	✗	✗	✗

Online Safety Act 2021

Online Content Scheme

Regulatory Guidance

eSC RG 4

Updated January 2025

Australian Government | eSafetyCommissioner

Contents

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public, online industry and other professionals who require further information about the Online Content Scheme. It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to address illegal and restricted online content. It also explains how eSafety will generally interpret and apply the law when responding to reports about illegal and restricted online content.

All decisions made by eSafety will be made on a case-by-case basis, considering the particular circumstances of each matter.

Overview of the Online Content Scheme

The Act includes an Online Content Scheme which has the following regulatory features:

1. A system under which a person can make a complaint about:

- online material that they believe to be illegal or should be restricted
- breaches of service provider rules and civil penalty provisions under the Online Content Scheme, and
- breaches of industry codes or standards.

2. Investigation and information gathering powers which allow eSafety to assess complaints, or investigate certain matters on our own initiative, and decide what action we can take.

3. Removal and restriction powers which allow eSafety to, in certain circumstances, give notices that direct online service providers to remove material (or remove access to material) from their services or ensure that access to certain types of material is restricted.

4. Powers to register industry codes and/or industry standards that regulate illegal and restricted online content.

5. Powers to determine service provider rules for certain online service providers.

6. Enforcement actions which are available to eSafety where there has been a failure to comply with our notices or other powers under the Online Content Scheme. These include seeking civil penalties for online service providers who fail to remove material in response to our notices.

7. Powers to apply to the Federal Court for an order to stop the provision of certain online services where the continued operation of the service represents a significant community safety risk.

Key terms

What is 'illegal and restricted online content'?

eSafety uses the term 'illegal and restricted online content' to refer to online content that ranges from the most seriously harmful material, such as videos showing the sexual abuse of children or which advocate terrorism, through to material which is inappropriate for children, such as online pornography.

The Act defines this content as either 'class 1 material'[1] or 'class 2 material'.[2] Class 1 material and class 2 material are defined by reference to Australia's National Classification Scheme, a cooperative arrangement between the Australian Government and state and territory governments for the classification of films, computer games and certain publications. For further information, see **Classification process on page 8**.

What is 'class 1 material' and 'class 2 material'?

Class 1 material is material[3] that is, or would likely be, refused classification 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.[4]

Class 2 material is material[5] that is, or would likely be, classified as either:

- X18+ (or, in the case of publications, category 2 restricted)[6], or
- R18+ (or, in the case of publications, category 1 restricted)[7]

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. For the purposes of this guidance, eSafety describes this as either class 2A material or class 2B material.

Class 2A material generally contains real sexual activity between consenting adults, where there is no violence, sexual violence or coercion and there are no fetishes or purposely demeaning activities. This material is generally known as 'pornography'.

[1]Section 106 of the Act. [2]Section 107 of the Act. [3]This material includes films, publications, computer games and any other material that is not a film, publication or computer game. [4]National Classification Code **https://www.legislation.gov.au/Details/F2013C00006**.
[5]This material includes films, publications, computer games and any other material that is not a film, publication or computer game. [6]Section 107(1)(a) – (e) of the Act. For the purposes of this guidance, eSafety refers to this material as class 2A material. [7]Section 107(1)(f) – (l) of the Act. For the purposes of this guidance, eSafety refers to this material as class 2B material.

Class 2B material can contain high impact depictions of simulated sexual activity, nudity, violence or drug use. It is considered unsuitable for children and young people under 18 years old.

	Material	National Classification Scheme
Class 1	Film Publication Computer game Any other material*	Refused Classification (RC)
Class 2A	Film Any other material (excluding computer games)*	X18+
	Publication	Category 2 restricted
Class 2B	Film Computer game Any other material*	R18+
	Publication	Category 1 restricted

*Under the Act, material that is not a film, computer game or publication is to be classified in a corresponding way to the way in which a film would be classified.

Context is important when classifying material. The nature and purpose of the material must be considered, including its literary, artistic or educational merit and whether it serves a medical, legal, social or scientific purpose.[8]

This means it is unlikely that sexual health education content, information about sexuality and gender, or health and safety information about drug use and sex will be considered illegal or restricted online content by eSafety.

What is 'child sexual exploitation material'?

Based on the ECPAT Terminology Guidelines (also known as the Luxembourg Guidelines),[9] the term 'child sexual exploitation material' is a broad category of content that encompasses material that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse.

Child sexual abuse material, which shows a sexual assault against a child, is a narrower category and can be considered a sub-set of child sexual exploitation material.

Class 1 material includes material that is both sexually exploitative and that depicts or describes child sexual abuse.

[8]Section 11 of the Classification (Publications, Films and Computer Games) Act 1995. [9]Interagency Working Group on Sexual Exploitation of Children, Luxemburg Guidelines, January 2016, **http://luxembourgguidelines.org/**.

What is a 'service provider rule'?

Under the Online Content Scheme, eSafety may introduce additional rules for providers of certain online services[10] where further legislative direction is required to support the regulation of class 1 material and class 2 material. For further information, see **Service provider determinations on page 19**.

What is a 'restricted access system'?

A restricted access system is a means of limiting access to material that is inappropriate for children and young people under 18. For further information, see **'When can eSafety issue a remedial notice?' on page 14**.

Making a complaint to eSafety

Who can complain?

A complaint under the Online Content Scheme can be made by:

- a person who resides in Australia
- a body corporate that carries on activities in Australia, which means a legal entity such as a company, or
- the Australian Government or one of its departments, or an Australian State or a Territory government or department.[11]

The complaint can be made to eSafety through the online form on our website..

What can a complaint cover?

A person may make a complaint to eSafety under the Online Content Scheme where they have reason to believe:

- service users in Australia can access class 1 material or class 2A material provided on a:
  - social media service
  - relevant electronic service, such as an email service, instant messaging service, SMS or MMS service, chat service or an online game where users can play with or against each other, or
  - designated internet service, such as a website[12]
- service users in Australia can access class 2B material provided on a social media service, a relevant electronic service or a designated internet service and access to the material is not subject to a restricted access system[13]
- an online service provider has breached a service provider rule[14]
- an online service provider has breached a civil penalty provision of the Online Content Scheme,[15] or
- an online service provider has breached an industry code or industry standard that applies to it.[16]

[10]This includes providers of social media services, relevant electronic services and designated internet services, as well as hosting service providers and internet service providers. [11]Section 41 of the Act. [12]Section 38(1) of the Act. [13]Section 38(2) of the Act. [14]Section 39(a) of the Act. [15]Section 39(b) of the Act. [16]Section 40 of the Act. Codes and standards will apply to providers of social media services, relevant electronic services, designated internet services, internet search engine services, app distribution services, internet carriage services and hosting services which host content in Australia, manufacturers and suppliers of equipment used by Australians to access online services, as well as those that install and maintain the equipment.

Where a complaint is made about class 1 or class 2 material, it should identify the service and location where the material can be accessed – this can be done, for example, by providing the full web address (or URL) for the material.

Investigations under the Online Content Scheme

eSafety may investigate various matters under the Online Content Scheme, either in response to a complaint or on our own initiative.[17] They include:

- whether users in Australia can access class 1 material provided on a social media service, designated internet service or relevant electronic service
- whether users in Australia can access class 2A material provided on a social media service, designated internet service or relevant electronic service
- whether users in Australia can access class 2B material provided on a social media service, designated internet service or relevant electronic service and, if so, whether the material is subject to a restricted access system
- whether an online service provider has breached a civil penalty provision under the Online Content Scheme (for example, if it has failed to comply with a removal notice for class 1 material)
- whether an industry participant has breached an industry code or industry standard that applies to it, and
- whether an online service provider has breached a Service Provider Rule that applies to it.

eSafety prioritises the investigation of complaints about the most harmful class 1 material. This includes child sexual exploitation material, material that advocates a terrorist act and material that promotes, instructs or incites in matters of crime and violence.

eSafety may ask for information from relevant people and online service providers and make any other enquiries that we think will help with our investigations into illegal or restricted online content.[18] eSafety's investigative powers are set out in Part 14 of the Act. Our powers include the ability to compel a person to answer questions and/or produce documents or other information.[19]

We have additional information-gathering powers under Part 13 of the Act to obtain identity and contact information for a service user from the provider of a social media service, relevant electronic service or designated internet service.[20] This information will be used to fulfill eSafety's functions under the Act, such as resolving a complaint. This power is not intended to be used by complainants to establish the identity of other service users.

Under the Act, eSafety may also refuse to investigate a complaint if it could have been made under an industry code or industry standard.[21] If eSafety refuses to investigate a matter, this decision is not subject to internal review or review by the Administrative Review Tribunal[#].

[17]Section 42 of the Act. [18]Section 42(3) of the Act. [19]Sections 197 to 205 of the Act. [20]Sections 193 to 196 of the Act. [21]Section 43 of the Act.

[#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).

Classification process

When considering illegal and restricted online content, eSafety must decide whether it would be defined as class 1 material or class 2 material. This is done by referring to the National Classification Scheme.

Under the Act, class 1 and class 2 materials are defined by reference to:

- the classification the material has received under the National Classification Scheme (where it has been classified), or
- eSafety's assessment of the classification the material would likely be given under the National Classification Scheme (where it has not been classified).

Under the Act, eSafety may make this assessment independently or may seek the advice of the Australian Classification Board to decide whether particular material would be class 1 material or class 2 material. eSafety might seek advice in situations where the likely classification of the material under the National Classification Scheme is uncertain.

Under the Classification (Publications, Films and Computer Games) Act 1995, the Classification Board is responsible for classifying films, computer games and some publications. Information about the Classification Board can be found at **www.classification.gov.au**. Advice provided by the Classification Board may be a relevant factor in any decision eSafety makes in relation to online material, but eSafety may also take other factors into account.

Referral of matters to law enforcement agencies

If eSafety considers particular material to be of a sufficiently serious nature to warrant referral to a law enforcement agency, eSafety must notify a member of an Australian police force.[22]

Sufficiently serious online material will ordinarily include material that:

- depicts or describes child sexual exploitation
- advocates a terrorist act, or
- promotes, incites or instructs in matters of crime.

eSafety has Memorandums of Understanding in place with the Australian Federal Police, and all State and Territory law enforcement agencies, to enable the fast referral of sufficiently serious material.

The Act also allows eSafety to refer sufficiently serious material to another person or body, where there is an agreement in place with the chief of an Australian police force that eSafety is authorised to do so.[23] An example of this arrangement is eSafety's membership of the **International Association of Internet Hotlines** (INHOPE), which allows for the referral of child sexual exploitation material between network members for rapid removal in the country where it is hosted. For further information, see **Informal requests on page 10**.

[22]Section 224(1) and specifically, 224(1)(b) of the Act. [23]Section 224(1)(d) of the Act.

Material that eSafety will not investigate

Under the Online Content Scheme, eSafety cannot investigate material that is, or would likely be, classified below R18+ (or, in the case of publications, category 1 restricted).

The Online Content Scheme does not provide eSafety with powers to address online issues such as copyright infringement, spam content, defamation and cybercrime, nor does the scheme provide eSafety with powers to investigate racist and discriminatory content, privacy issues or online scams. Information about alternative reporting pathways for these issues is available on the **eSafety website**.

While eSafety investigates and helps remove online child sexual exploitation material, our notice powers do not extend to address the creation of the material or the sexual exploitation of children – these are police matters. Any instances of online child sexual exploitation, including inappropriate online contact, suspected grooming by sexual predators or procurement of children over the internet should be reported to the **Australian Centre to Counter Child Exploitation** led by the Australian Federal Police.

Approaches to compliance – illegal and restricted online content

Under the Act, eSafety can consider a range of informal and formal compliance options when seeking to remove or limit access to illegal and restricted online content.

Factors we may take into account include:

- the harm or likely harm from production of the material (for example, to victims of child sexual exploitation or violent crime)
- the harm or likely harm from consumption of the material (for example, normalising child sexual exploitation by allowing access to and sharing of images and videos of children being sexually abused)
- the harm or likely harm to victims from the distribution of the material (for example, retraumatising or further compounding the trauma experienced by the victims harmed in the production of the content.
- whether other options exist to limit access to the material (for example, device-level filtering software or parental control tools)
- the context in which the material is presented (for example, content that is presented in a factual and objective way intended to contribute to public debate may be regarded as having a lower impact than the same material presented without contextual justification), and
- any other factors that eSafety considers to be of relevance.

eSafety may also consider these factors when determining which, if any, compliance or enforcement action to take. Further factors that eSafety may consider are set out in **eSafety's Compliance and Enforcement Policy**.

Informal requests

eSafety often approaches online service providers informally to ask them to remove class 1 or class 2 material in the first instance. Informal requests often lead to faster removal of the material compared to formal action, resulting in fewer Australians being exposed to harmful online content.

Additionally, where there are established reporting pathways for the removal of online child sexual exploitation material, eSafety will prefer them over taking formal action.

For example, eSafety is the Australian hotline member of **INHOPE**, a global network of organisations dedicated to the rapid removal of online child sexual exploitation material. All hotline members have established relationships with the online industry and law enforcement agencies in their own country, which means that the removal of reported material can be actioned much faster than if we chose to give a removal notice.

Reporting to INHOPE is enabled by a memorandum of understanding with the Australian Centre to Counter Child Exploitation. Under the memorandum of understanding, eSafety notifies INHOPE in relation to child sexual exploitation material in a member country, rather than giving a formal notice or referring the matter to Australian law enforcement.

Formal actions

While eSafety prefers to seek informal removal of material by online service providers, we do not hesitate to use our formal powers where we consider it appropriate.

For example, if an online service provider has a history of not responding to our informal requests or there are other factors that suggest an online service provider is unlikely to respond to an informal request, eSafety may decide to give a removal notice without first approaching the provider informally.

eSafety is aware that some online service providers may prefer to receive a formal notice to qualify for certain protections set out under section 221 of the Act. If this is the case, eSafety's preference is that this be made clear in the response to an informal request so we can assess the appropriateness of formal action as quickly as possible.

Compliance options

Under the Act, eSafety can consider a range of formal compliance options in relation to class 1 and class 2 material.

Action	Outcome	Class 1	Class 2A	Class 2B
Give a service provider notification	Put an online service provider on notice	✓	✓	✓
Give a removal notice	Require removal of material	✓	✓	
Give a remedial notice	Require removal of material or access to material to be restricted			✓
Give a link deletion notice	Require removal of access to material	✓		
Give an app removal notice		✓		

eSafety prioritises the removal of class 1 material over class 2 material as class 1 is the most harmful. For more information, please see **eSafety's Compliance and Enforcement Policy**.

Service provider notifications

What are service provider notifications?

Generally, a service provider notification is a written notice that informs an online service provider that eSafety is aware of illegal or restricted online content on its service.

A service provider notification may be given to the provider of a social media service, a relevant electronic service or a designated internet service[24] that is not exempt under the Act.[25]

When can eSafety give a service provider notification under the Online Content Scheme?

A service provider notification can be given in relation to class 1 material or class 2 material.

Class 1 material: A service provider notification can be given where eSafety is satisfied that all of the following are true:

- class 1 material is, or has been, provided on a social media service, relevant electronic service or designated internet service (which is not an exempt service) on two or more occasions during the past 12 months
- the material can be, or was able to be, accessed by service users in Australia, and
- the provision of the material contravened the service's terms of use.[26]

[24]Sections 113A, 118A and 123A of the Act. [25]Exempt services are: an exempt Parliamentary content service, an exempt court/tribunal content service and an exempt official inquiry content service. These are defined in section 5 of the Act. [26]Section 113A of the Act.

Class 2A material: A service provider notification can be given where eSafety is satisfied that all of the following are true:

- class 2A material is, or has been, provided on a social media service, relevant electronic service or designated internet service (which is not an exempt service) on two or more occasions during the past 12 months
- the material can be, or was able to be, accessed by service users in Australia the service is provided from Australia, and
- the provision of the material contravened the service's terms of use.[27]

Class 2B material: A service provider notification can be given where eSafety is satisfied that all of the following are true:

- class 2B material is, or has been, provided on a social media service, relevant electronic service or a designated internet service (which is not an exempt service) on two or more occasions during the past 12 months
- the material can be, or was able to be, accessed by service users in Australia
- access to the material is not, or was not, subject to a restricted access system
- the service is provided from Australia, and
- the provision of the material contravened the service's terms of use.[28]

eSafety may also publish any service provider notification on our website. The purpose of publishing this notification is to call out services that are not doing enough to combat class 1 and class 2 material.[29]

What are the consequences of a service provider notification?

A service provider notification is a less formal approach than issuing a removal notice and there is no enforcement action which arises from a failure to act after receiving such a notification.

However, eSafety will consider an online service provider's response to any such notifications when considering other regulatory options.

Removal notices

What is a removal notice?

A removal notice is a written notice requiring the recipient to take all reasonable steps to remove class 1 material or class 2A material from a service within 24 hours or a longer timeframe specified by eSafety.

A removal notice may be given to the provider of a social media service, a relevant electronic service, a designated internet service,[30] or a hosting service that is not exempt under the Act.[31]

[27]Section 118A of the Act. [28]Section 123A of the Act. [29]Sections 113A, 118A and 123A of the Act.
[30]Section 109 and 114 of the Act. [31]Section 110 and 115 the Act.

When can eSafety issue a removal notice under the Online Content Scheme?

Under the Online Content Scheme, eSafety may give a removal notice for class 1 material or class 2A material.

For class 1 material, the removal notice may be given if all of the following are true:

- the material is, or has been, provided on a social media service, a relevant electronic service, or a designated internet service that is not exempt under the Act[32]
- eSafety is satisfied that the material is, or was, class 1 material, and
- the material can be accessed by service users in Australia.[33]

If all these criteria are met, a removal notice can also be given to the hosting service provider that hosts the material.[34]

For class 2A material, the removal notice may be given if all of the following are true:

- the material is, or has been provided on a social media service, a relevant electronic service, or a designated internet service that is not exempt under the Act[35]
- eSafety is satisfied that the material is, or was, class 2A material
- the material can be accessed by service users in Australia, and
- the online service is provided from Australia.[36]

When considering whether a service is 'provided from Australia' eSafety will take into account factors such as whether the online service is being hosted in Australia, or whether the online service provider has a registered Australian business presence (for example, if it has an Australian Business Number or an Australian Company Number). There may be other factors which indicate that an online service is provided from Australia.

A removal notice can also be given to a hosting service provider where the class 2A material is, or has been, provided on a social media service, relevant electronic or designated internet service (which is not an exempt service), the material can be accessed by service users in Australia and the material is hosted by a hosting service provider in Australia.[37]

For both class 1 material and class 2A material, the Act does not impose any time limits within which a removal notice must be given.

The giving of a removal notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. This may also include a decision to revoke a removal notice after it is given.[38]

[32]Exempt services are: an exempt Parliamentary content service, an exempt court/tribunal content service and an exempt official inquiry content service. These are defined in section 5 of the Act. [33]Section 109(1) of the Act. [34]Section 110(1) of the Act. [35]Exempt services are: an exempt Parliamentary content service, an exempt court/tribunal content service and an exempt official inquiry content service. These are defined in section 5 of the Act. [36]Section 114(1) of the Act. [37]Section 115(1) of the Act. [38]Section 113 of the Act.

What are the consequences of a removal notice?

An online service provider must comply with a requirement under a removal notice for class 1 material or class 2A material to the extent that it is capable of doing so.

Failure to comply with a removal notice may result in a civil penalty of up to 500 penalty units.[39] eSafety may also consider several other enforcement options.

Remedial notices

What is a remedial notice?

A remedial notice is a written notice requiring the recipient to take all reasonable steps to remove class 2B material from a service, or place the material behind a restricted access system, within 24 hours or a longer timeframe specified by eSafety.

A remedial notice may be given to the provider of a social media service, a relevant electronic service, a designated internet service,[40] or a hosting service that is not exempt under the Act.[41]

When can eSafety issue a remedial notice?

Under the Online Content Scheme, eSafety may give a remedial notice for class 2B material if all of the following are true:

- the material is, or has been provided on a social media service, a relevant electronic service, or a designated internet service that is not exempt under the Act[42]
- eSafety is satisfied that the material is, or was, class 2B material
- the material can be accessed by service users in Australia, and
- the online service is provided from Australia.[43]

A remedial notice can also be given to a hosting service provider where the class 2B material is, or has been, provided on a social media service, relevant electronic or designated internet service (which is not an exempt service), the material can be accessed by service users in Australia and the material is hosted by a hosting service provider in Australia.[44]

A restricted access system is a means of limiting access to material that is inappropriate for children and young people under 18 years old. The Act empowers eSafety to declare what constitutes a restricted access system for the purposes of the Act. This is set out in the Restricted Access System Declaration and supporting Explanatory Statement.

The Act does not impose any time limits within which a remedial notice must be given.

The issuing of a remedial notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. This may also include a decision to revoke a remedial notice after it is issued.[45]

[39]Section 111 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. [40]Section 119 of the Act. [41]Section 120 of the Act. [42]Exempt services are: an exempt Parliamentary content service, an exempt court/tribunal content service and an exempt official inquiry content service. These are defined in section 5 of the Act. [43]Section 119(1) of the Act. [44]Section 120(1) of the Act. [45]Section 123 of the Act.

What are the consequences of a remedial notice?

A service must comply with a requirement under a remedial notice for class 2B material to the extent that that it is capable of doing so.

Failure to comply with a remedial notice may result in a civil penalty of up to 500 penalty units.[46] eSafety may also consider several other enforcement options.

Link deletion notice

What is a link deletion notice?

A link deletion notice is a written notice requiring the recipient to stop providing a link that gives Australian service users access to class 1 material within 24 hours or a longer timeframe specified by eSafety.

A link deletion notice can only be given to a provider of an internet search engine service.[47]

When can eSafety issue a link deletion notice?

Under the Online Content Scheme, eSafety may give a link deletion notice if all of the following are true:

- a person provides an internet search engine service
- users in Australia can access class 1 material using a link provided by the internet search engine service[48]
- there were two or more times in the past 12 months when users in Australia could access class 1 material using a link provided by the service, and
- during the past 12 months, eSafety gave one or more removal notices in relation to class 1 material that could be accessed using a link provided by the service, and those removal notices were not complied with.[49]

The Act does not impose any time limits within which a link deletion notice must be given.

Giving a link deletion notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. This may also include a decision to revoke a link deletion notice after it is given.[50]

What are the consequences of a link deletion notice?

A person must comply with a requirement under a link deletion notice to the extent that they are capable of doing so.

Failure to comply with a link deletion notice may result in a civil penalty of up to 500 penalty units.[51] eSafety may also consider several other enforcement options.

[46]Section 121 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. [47]Section 124 of the Act. [48]Section 124(1) of the Act. [49]Section 124(1) of the Act. [50]Section 127 of the Act. [51]Section 125 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual.

App removal notice

What is an app removal notice?

An app removal notice is a written notice requiring the recipient to remove an app, including a computer program, that provides access to class 1 material from a service within 24 hours or a longer timeframe specified by eSafety.

An app removal notice can only be given to a provider of an app distribution service.[52]

When can eSafety issue an app removal notice?

Under the Online Content Scheme, eSafety may give an app removal notice if:

- a person provides an app distribution service
- the service enables users in Australia to download an app that facilitates the posting, sharing or sending of class 1 material on a social media service, relevant electronic service or a designated internet service[53]
- eSafety is satisfied that there were two or more times during the past 12 months when users in Australia could use the service to download an app that facilitates the posting, sharing or sending of class 1 material, and
- during the past 12 months, eSafety issued one or more removal notices in relation to class 1 material, the posting, sharing or sending of which is facilitated by the app, and those removal notices were not complied with.[54]

The Act does not impose any time limits within which an app removal notice must be given.

Giving an app removal notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. This may also include a decision to revoke an app removal notice after it is given.[55]

What are the consequences of an app removal notice?

A person must comply with a requirement under an app removal notice to the extent that they are capable of doing so.

Failure to comply with an app removal notice may result in a civil penalty of up to 500 penalty units.[56] eSafety may also consider several other enforcement options.

[52]Section 128 of the Act. [53]Section 128(1) of the Act. [54]Section 128(4) of the Act.
[55]Section 131 of the Act. [56]Section 129 of the Act.

Approaches to compliance - industry codes and standards

In addition to eSafety's removal powers, the Act provides for industry codes or industry standards to be developed to regulate class 1 and class 2 material.[57] Codes are to be developed by industry bodies or associations and registered by eSafety,[58] while eSafety is responsible for drafting and registering industry standards.[59]

Codes or standards will apply to the participants of eight key sections of the online industry that provide a wide range of services to Australians. These include:

- social media services
- relevant electronic services
- designated internet services
- internet search engine services
- app distribution services
- internet carriage services
- hosting services which host content in Australia
- manufacturers and suppliers of equipment used by Australians to access online services, as well as those that install and maintain the equipment.[60]

eSafety can receive complaints and investigate potential breaches of the codes or standards.[61] Breaches will be enforceable by civil penalties and other enforcement options.[62]

The Act provides a list of examples of matters that may be dealt with by industry codes and standards.[63]

Industry codes

In September 2021, eSafety released a position paper which outlined eSafety's expectations for the development of industry codes by industry bodies and associations. It outlined our preferred outcomes-based model for the codes and the two-phase approach to codes development. The first phase of codes focused on class 1 material and the second phase will focus on class 2 material.

The Act empowers eSafety to register the codes that are submitted by industry associations if they meet the statutory requirements.[64]

Once a code is registered in accordance with the Act, eSafety may direct compliance with the code. Failure to comply with a written direction to comply with the code may attract a civil penalty of up to 500 penalty units.[65] eSafety may also consider several other enforcement options.

[57]Sections 132 to 142 and 145 of the Act. [58]Section 140 of the Act. [59]Section 145 of the Act. [60]Section 135 of the Act.
[61]Sections 40 and 42 of the Act. [62]Sections 143, 144, 146 and 147 of the Act. [63]Section 138 of the Act. [64]Section 140 of the Act.
[65]Section 146 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual.

Industry standards

eSafety has the power under the Act to determine industry standards when:

- eSafety has made a request for code development under the Act that is not complied with or one of a number of other conditions are satisfied, including that a draft code does not contain appropriate community safeguards for matters specified in eSafety's request for its development
- eSafety has published a notice stating that if an industry body or association were to come into effect, eSafety would likely request that body or association develop a code and no industry body or association comes into existence within the period specified, or
- eSafety is satisfied that a code that has been registered for at least 180 days is deficient, has notified the body or association of the deficiencies and requested that they be addressed, and the notified deficiencies have not been adequately addressed within a specified period.[66]

In addition, eSafety must not determine a standard unless satisfied that it is necessary or convenient to provide appropriate community safeguards or otherwise adequately regulate participants in a section of the online industry.[67]

Failure to comply with an industry standard may attract a civil penalty of up to 500 penalty units.[68] eSafety may also consider several other enforcement options.

Industry standards for the RES and DIS sections of the online industry are being prepared by eSafety in the second half of 2023.

Additional codes and/or standards will also be prepared to address class 2 content. All industry codes and standards will be available on **eSafety's register of industry codes and standards** once they are in place.

[66]Section 145 of the Act. [67]Section 145(1B) of the Act. [68]Section 146 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual.

Approaches to compliance - service provider determinations

Under the Online Content Scheme, eSafety may introduce additional rules for providers of certain online services, where further legislative direction is required to support the regulation of class 1 and class 2 material.[69]

If made, the additional rules (known as 'service provider rules') would be set out in a legislative instrument known as a 'service provider determination'.

Service provider determinations can be made in relation to the providers of:

- social media services
- relevant electronic services
- designated internet services
- hosting services
- internet carriage services.[70]

Failure to comply with a service provider rule may result in a civil penalty of up to 500 penalty units.[71] eSafety may also consider additional enforcement actions, including remedial directions and formal warnings.[72] Failure to comply with a remedial direction may result in a civil penalty of up to 500 penalty units.[73]

The relevant portfolio minister may also, by legislative instrument, declare that a specified service provider is exempt from all or specific service provider rules.[74]

[69]Section 151 of the Act. [70]Section 151(1) of the Act. [71]Section 153 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. [72]Sections 154 and 155 of the Act. [73]Section 154(4) of the Act. [74]Section 152 of the Act.

Taking enforcement action

eSafety is empowered under the Act to address class 1 and class 2 material through a range of actions. Where appropriate, eSafety takes a graduated approach to enforcement.

Enforcement options include the following:

- **Formal warnings**. A formal warning can be issued to advise an online service provider that they have failed to comply with the requirements of a removal notice, a remedial notice, a link deletion notice, an app deletion notice, an industry standard, an industry code or a service provider rule.
- **Enforceable undertakings**. An online service provider may enter into an agreement with eSafety to ensure compliance with the Online Content Scheme requirements. Once accepted by eSafety, the undertaking can be enforced by a Court. For the purposes of the Online Content Scheme, an enforceable undertaking is available where a service has failed to comply with a removal notice, a remedial notice, a link deletion notice, an app deletion notice, an industry standard or a direction to comply with an industry code.[75]
- **Injunctions**. An injunction is an order granted by a Court to compel an online service provider to take certain actions, or to refrain from taking certain actions, to comply with the Online Content Scheme requirements. For the purposes of the Online Content scheme, an injunction is available when a service has failed to comply with a removal notice, a remedial notice, a link deletion notice, an app deletion notice, an industry standard or a direction to comply with an industry code.[76]
- **Infringement notices**. Infringement notices are notices that set out the particulars of an alleged contravention and specify an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings. For the purposes of the Online Content Scheme, an infringement notice is available when a service has failed to comply with a removal notice, a remedial notice, a link deletion notice, an app deletion notice, or a direction to comply with an industry code or an industry standard.[77] Infringement notices may be issued by eSafety and do not require the involvement of a court.[78]
- **Civil penalty orders**. These are court orders that require a person who is found to have contravened a civil penalty provision of the Act to pay a penalty. For the purposes of the Online Content Scheme, these orders can be sought for each of the reasons that eSafety may issue an infringement notice as well as a failure to comply with a service provider rule.[79]

[75]Section 164(1) of the Act. [76]Section 165(1) of the Act. [77]Section 163(1) of the Act. [78]Subject to requirements in the Regulatory Powers (Standard Provisions) Act 2014. [79]Section 162 of the Act.

Orders to cease a service

In the most extreme circumstances, eSafety may apply to the Federal Court to order that the provider of a particular social media service,[80] relevant electronic service[81] or designated internet service[82] stop providing that service in Australia, or for the supplier of an internet carriage service to stop supplying that service in Australia.[83]

Making such an application is a very serious step, and one that eSafety would consider only as a last resort where a service poses a serious threat to the safety of Australians.

Before making an application, eSafety must be satisfied that the service failed to comply with a civil penalty provision under the Online Content Scheme (such as a class 1 removal notice) on two or more occasions over the past 12 months. In addition, eSafety must be satisfied that, as a result of those failures to comply, the continued operation of the service poses a significant community safety risk.

Before making an order on the basis of that application, the Federal Court must also be satisfied that the service failed to comply with a civil penalty provision under the Online Content Scheme (such as a class 1 removal notice) on two or more occasions over the past 12 months. In addition, the Federal Court must also be satisfied that, as a result of those failures to comply, the continued operation of the service poses a significant community safety risk.

[80]Section 156 of the Act. [81]Section 157 of the Act. [82]Section 158 of the Act. [83]Section 159 of the Act.

Review rights

Certain actions taken by eSafety under the Online Content Scheme can be reviewed internally by eSafety and externally by the Administrative Review Tribunal[#]. The purpose of these review rights is to ensure that we have made the correct and preferable decision on a case-by-case basis.

Under the Online Content Scheme, a review can be requested where:

- a removal notice, a remedial notice, a link deletion notice or an app removal notice has been given
- eSafety decides to give or vary a direction to comply with an industry code or refuses to revoke the direction
- eSafety decides to give or vary a remedial direction to ensure compliance with a service provider rule or refuses to revoke the direction
- eSafety has made a decision of an administrative nature under a service provider determination, or
- eSafety refuses to register an industry code, where the body or association that develops the code requests the review.

Basic Online Safety Expectations

The Basic Online Safety Expectations (the Expectations) are a set of expectations set by the Australian Government for social media services, relevant electronic services and designated internet services. eSafety can require providers of these kinds of services to report on how they are meeting the Expectations.

The Expectations are focused on ensuring that these services take reasonable steps to keep Australian end-users safe including in relation to illegal and restricted online content. They also aim to provide greater transparency and accountability around services' safety features, policies and practices. More information about the Expectations and how eSafety uses its powers to require transparency in relation to them can be found in the Basic Online Safety Expectations regulatory guidance on **eSafety's website**.

Find more information and support

For more information regarding illegal and restricted online content, or to make a complaint about illegal and restricted online content to eSafety, please visit our website at **eSafety.gov.au**.

If you are in Australia and you are in immediate danger, call police on Triple Zero (000). If you are 25 or under and need support, you can call Kids Helpline anytime on 1800 55 1800. If you are 25 or over, please call Lifeline on 13 11 14.

[#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).

Published: January 2025 (Updated)

Online Safety Act 2021

Cyberbullying Scheme
Regulatory Guidance
eSC RG 1

Updated January 2025

Australian Government | eSafetyCommissioner

Contents

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public (including children, parents, carers and educators), online industry and other professionals who require further information about the Cyberbullying Scheme. It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to address cyberbullying of Australian children. It also explains how eSafety will generally interpret and apply the law when responding to reports of cyberbullying.

All decisions made by eSafety will be made on a case-by-case basis, considering the particular circumstances of each complaint received.

Overview of the Cyberbullying Scheme

The Cyberbullying Scheme is a safety net to be used when a complaint has been made to an online service provider but the online service provider has not removed the material. The Cyberbullying Scheme has the following regulatory features:

1. **A system under which a person may make a complaint to eSafety** about cyberbullying material that targets an Australian child. The complainant must have first reported the material to the relevant online service provider before asking eSafety to give a notice to the provider requiring removal of the cyberbullying material.

2. **Investigative and information gathering powers** which allow eSafety to assess complaints about cyberbullying material targeting an Australian child and decide what action we can take.

3. **Removal powers** which allow eSafety to give notices to online service providers, and to people (end-users) who have posted, shared or sent cyberbullying material, requiring them to remove the material. Notices to end-users can also require that the person stop posting, sharing or sending cyberbullying material directed to the targeted child and apologise to them.

4. **Enforcement actions** available to eSafety where there has been a failure to comply with our notices. These range from issuing a formal warning to seeking civil penalties.

Key terms

Who is 'an Australian child'?

When the Act refers to 'an Australian child' it generally means any young person under 18 who ordinarily lives in Australia. This can include an Australian child who is travelling overseas temporarily.

eSafety cannot use its powers under the Cyberbullying Scheme to help a child who does not ordinarily live in Australia.

What is 'cyberbullying material'?

Under the Act, cyberbullying material[2] means online communication to or about an Australian child that is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating. It can include posts, comments, emails, messages, memes, images and videos.

For eSafety to investigate, the material must target a specific child, not broad groups of unidentified children.

What is 'seriously threatening, seriously intimidating, seriously harassing, or seriously humiliating' material?

These terms are not defined in the Act and are intended to have their ordinary meaning. Cyberbullying material will not generally include material that is simply offensive or insulting.

Examples include:

1. **Seriously threatening:** when someone posts or comments that they are going to harm a child, or encourages others to do it, such as saying 'We're going to wait outside your house and bash you when you come out' or 'If you stop talking to me I will post your address and phone number all over the internet.'

2. **Seriously intimidating:** when someone posts something that is designed to make the child fearful but is not on its face a direct threat, e.g. posting an image showing a person with their head in a guillotine with the caption "Snitches get stitches" and tagging the child.

3. **Seriously harassing:** when someone keeps sending messages to a child or persistently reposting material. Each message or post on its own may not be enough to be called cyberbullying material, but the repetition increases the impact.

4. **Seriously humiliating:** when someone posts a comment or shares an image that seriously embarrasses a child – this could be a video that shows a child with a mobility disability slipping in mud at school then crying about having to wear dirty clothes all day, with captions and comments making fun of the child's disability and how the child 'can't even walk properly'.

[1]Section 5 of the Act. [2]Section 6 of the Act. [3]Section 6(4) of the Act.

Is any material exempt from cyberbullying complaints?

The Act recognises that a person in a position of authority over a child (such as their parent, carer, teacher or employer) may need to send, post or share material that could upset the child. If this action is considered reasonable in the circumstances, it will not be treated by eSafety as cyberbullying. For example, if a teacher posts class exam results online or an employer emails a young person to notify them of their dismissal, neither of those materials would meet the definition of cyberbullying.

Making a complaint to eSafety

Who can complain?

A cyberbullying complaint may be made to eSafety by the targeted child, a parent or guardian of the child or someone who is authorised by the child to complain on their behalf. The complaint can be made to eSafety through the online form on our website.

Complaint made by an Australian child

A cyberbullying complaint may be made by an Australian child if they have reason to believe they are, or have been, the target of cyberbullying material.[4]

The material must be, or have been, provided on:

- a social media service
- a relevant electronic service such as an email service, chat service, instant messaging service or an online game where end-users play against each other, or
- a designated internet service such as a website or app.

A person who has recently turned 18 can complain about cyberbullying material that targeted them before they turned 18 if both of the following additional conditions are met:

- the complaint is made within a reasonable time after the person became aware of the material; and
- the complaint is made within 6 months after the person reached 18 years of age.[5]

Complaint made on behalf of an Australian child

A responsible person may make a complaint on behalf of an Australian child if the person has reason to believe that the child is, or has been, the target of cyberbullying material on one of the online services listed in the previous section. This person can be a parent or guardian of the child, or a responsible person the child has asked to make a complaint about the matter – for example, this could be a family member, carer, friend, teacher or police officer.[6]

Making a complaint to online service providers first

If the person making the complaint wants eSafety to give a removal notice to an online service provider, they must show that they have made a complaint about the material to the relevant online service provider listed in the previous section. We will ask for this evidence through our online reporting form. eSafety cannot give a removal notice until at least 48 hours have passed since the complaint was made to the relevant online service provider.

[4]Section 30(1) of the Act. [5]Section 30(3) of the Act. [6]Section 30(2) of the Act. [7]Section 30(4) of the Act.

Many online services provide links or other methods for members of the public to report cyberbullying and they will have the material removed without help from eSafety. This is often the fastest way to get material removed. The **eSafety Guide** has more information about how to report cyberbullying to commonly used online services.

If the relevant online service provider supplies a receipt, reference or report number as part of its business processes, we will usually need to know that number. In cases where receipts are not provided, we will need a screenshot of the report or some other proof that it was made. Otherwise, a statutory declaration can be supplied – this is a legal document that contains a written statement saying something is true, which has been witnessed by an authorised person.

Investigation of cyberbullying material

Under the Act, eSafety is empowered to investigate complaints about cyberbullying material.[8]

eSafety may ask for information from relevant people, organisations and online service providers, and make any other enquiries that will help with our investigation of a cyberbullying complaint. eSafety may also end an investigation at any point.[10]

eSafety's investigative powers are set out in Part 14 of the Act. These powers include the ability to compel a person to answer questions and/or produce documents or other information.[11] eSafety has additional information-gathering powers under Part 13 of the Act to obtain end-user identity and contact information from the provider of a social media service, relevant electronic service or designated internet service.[12]

Approaches to compliance and enforcement

When seeking to have cyberbullying material removed, eSafety may take informal or formal action.

Informal requests

eSafety often approaches online service providers informally to ask them to remove cyberbullying material in the first instance. We find that this generally results in faster removal of material compared to formal action, which is a better outcome for the targeted child.

Formal actions

While eSafety will generally seek informal removal of material by online service providers, we will not hesitate to use our formal powers when we consider it appropriate.

For example, if an online service provider has a history of not responding to our informal removal requests or there are other factors that suggest the online service provider is unlikely to respond to an informal removal request, we may decide to give a removal notice without first approaching them informally for removal.

[8]Section 31(1) of the Act. [9]Section 31(2) of the Act. [10]Section 31(5) of the Act. [11]Sections 197 to 205 of the Act. [12]Sections 193 to 196 of the Act.

Some online service providers and end-users may prefer to receive a formal notice from eSafety, which means certain legal protections set out under section 221 of the Act will apply. If this is the case, eSafety's preference is that the online service provider make this clear in their response to an informal request so eSafety can assess the appropriateness of formal action as quickly as possible.

Compliance and enforcement options

Under the Act, eSafety can consider a range of formal compliance and enforcement options when investigating cyberbullying material.

Outcome	**Formal action** - directed towards end-users	**Formal action** - directed towards online service providers
Put an online service provider on notice		Give one of the following **service provider notifications**: • a written notice informing an online service provider that material that meets the definition of cyberbullying is on its service • a statement informing an online service provider that material that meets the definition of cyberbullying and that breaches the service's own terms of use is, or was, on its service on two or more occasions over the past 12 months. In addition, eSafety may publish this statement on our website.
Require removal of content	Give an **end-user notice** requiring the person who posted, shared or sent the cyberbullying material to do any or all of the following: • take all reasonable steps to ensure the removal of the material within a timeframe specified by eSafety • stop posting, sharing or sending cyberbullying material targeting the child • apologise to the child in a way and timeframe specified by eSafety (or if the child has become an adult, to the adult). This can be given where eSafety has received a valid complaint and eSafety is satisfied a complaint has been made about the material to the relevant online service provider.	Give a **removal notice to an online service provider** requiring the online service provider to remove the material on the service or take all reasonable steps to cease hosting the material within 24 hours (or a longer timeframe if allowed by eSafety). This can be given where a valid complaint has been received by eSafety and eSafety is satisfied a complaint has been made about the material to the relevant online service provider and removal has not occurred within 48 hours.
Take enforcement action	Options where an end-user fails to comply with a requirement under an end-user notice: • issuing a formal warning • seeking a court injunction.	Options where a service provider fails to comply with a requirement under a removal notice: • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order.

Service provider notifications

What are service provider notifications?

Generally, a service provider notification informs the online service provider that eSafety is aware that material which meets the definition of cyberbullying is on its service.

A service provider notification may be given to the provider of a social media service, relevant electronic service or designated internet service.[13]

eSafety can issue two different types of service provider notifications, as set out in the next section.

When can eSafety give a service provider notification under the Cyberbullying Scheme?

Service provider notifications can be given in two circumstances:

- eSafety may give a written notice to an online service provider to make it aware of cyberbullying material on its service following a complaint. We can give this notice to an online service provider even if a complainant has not yet made a complaint about the matter to the online service provider. This is a quick way of putting the service provider "on notice" about cyberbullying material, and eSafety expects the notice would prompt the service provider to remove the material. eSafety may use this option where, for example, a less formal approach is likely to result in faster content removal. This type of service provider notification can only be given with the consent of the complainant and does not give rise to enforcement options if the online service provider does nothing in response.[14]
- If cyberbullying material is, or was, available on an online service provider on two or more occasions over the past 12 months, eSafety may:
  - prepare a statement to that effect, and
  - publish the statement on our website and
  - give a copy of the statement to the online service provider.

    To give this statement, the material must also have breached the service's own terms of use. The purpose of publishing this statement is to call out services that are not doing enough to combat cyberbullying.[15] eSafety will generally give an online service provider a chance to comment (and take action) before determining whether to publish the statement.

[13]Section 73 of the Act. [14]Section 73(1) of the Act. [15]Section 73(2) of the Act.

What are the consequences of a service provider notification?

A service provider notification is a less formal approach than giving a removal notice and there is no enforcement action which arises from a failure to act after receiving such a notification.

However, eSafety expects that an online service provider would take action to remove the content without the need for eSafety to give a removal notice.

In addition, eSafety will consider an online service provider's response to any notifications when considering other regulatory options.

Removal notices

What is a removal notice?

A removal notice is a written notice requiring the recipient to remove or take all reasonable steps to cease hosting the cyberbullying material from a service within 24 hours or a longer timeframe specified by eSafety.

A removal notice may be given to the provider of a social media service, relevant electronic service, designated internet service,[16] or hosting service.[17]

Failure to comply with the notice enables eSafety to take a range of enforcement actions, from issuing a formal warning to seeking civil penalty orders.

When can eSafety issue a removal notice under the Cyberbullying Scheme?

eSafety may give a removal notice where:

- a complaint has been made to eSafety about the material
- the material is, or has been, provided on a social media service, a relevant electronic service or a designated internet service
- the material was the subject of a complaint made to the provider of the service
- the material was not removed from the service within 48 hours after the complaint was made or such longer period as eSafety allows
- eSafety is satisfied that the material is, or was, cyberbullying material targeted at an Australian child, and
- the material can be identified in a way that enables the online service provider or end-user to comply with the notice such as for example through screenshots, URLs, usernames or time stamps.[18]

A removal notice can also be given to a hosting service provider where the material provided on a social media service, relevant electronic or designated internet service is hosted by a hosting service provider and the criteria listed in this section are met.[19]

The Act does not impose any time limits within which a removal notice must be given.

The giving of a removal notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action.

[16]Section 65 of the Act. [17]Section 66 of the Act. [18]Sections 65 and 66 of the Act. [19]Section 66 of the Act.

What are the consequences of a removal notice?

A person must comply with a requirement under a removal notice to the extent that the person is capable of doing so.[20]

Failure to comply with a removal notice may result in a civil penalty of up to 500 penalty units.[21] eSafety may also consider several other enforcement options.

End-user notices

What is an end-user notice?

An end-user notice is a written notice to an end-user requiring them to do any or all of the following:

- take all reasonable steps to ensure the removal of the cyberbullying material from a specified service, and do so within the period specified in the notice
- refrain from posting, sharing or sending cyberbullying material directed at the targeted child, and
- apologise to the child (or, if the child has become an adult, to the adult) for posting, sharing or sending the material and to do so within the period specified in the notice.[22]

When can eSafety issue an end-user notice?

eSafety can issue an end-user notice when:

- the material is, or has been, provided on a social media service, a relevant electronic service or a designated internet service
- a complaint has been made to eSafety about the material
- eSafety is satisfied that the material is, or was, cyberbullying material targeted at an Australian child, and
- the material was posted, shared or sent on the service by a particular end-user of the service.[23]

The Act does not impose any time limits within which an end-user notice must be given.

The giving of an end-user notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether we will take action.

eSafety will typically work with the school principal or head teacher of the end-user's school in order to serve such a notice. When a school recognises the role they can provide in encouraging accountability and are willing to be part of a solution to address these behaviours, this route provides eSafety with the most effective way to disrupt a student's cyberbullying behaviour permanently, even if the target of the end-user's behaviour is not at the same school.

eSafety will work with schools to ensure that the end-user is appropriately supported and educated on what constitutes cyberbullying and the need to refrain from posting further cyberbullying material.

[20]Section 67 of the Act. [21]The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. [22]Section 70 of the Act. [23]Section 70 of the Act. [24]Section 71 of the Act.

What are the consequences of failing to comply with an end-user notice?

A person must comply with a requirement under an end-user notice to the extent that the person is capable of doing so.[24]

Where a person fails to comply with an end-user notice, eSafety can take injunctive action or issue a formal warning.

Taking enforcement action

Sometimes eSafety needs to go a step further, taking enforcement action against an end-user who has failed to comply with an end-user notice, or an online service provider who has failed to comply with a removal notice.

eSafety is empowered under the Act to address cyberbullying material through a range of actions. Where appropriate, eSafety takes a graduated approach to enforcement action.

Enforcement options available include the following:

- **Formal warnings**. A formal warning can be issued to either:
  - advise an online service provider that they have failed to comply with the requirements of a removal notice, and they could face further consequences if they continue to fail to comply, or
  - advise an end-user that they have failed to comply with the requirements of an end-user notice and they could face further consequences if they continue to fail to comply.
- **Enforceable undertakings**. An enforceable undertaking requires an online service provider to enter into an agreement with eSafety to ensure compliance with the Cyberbullying Scheme requirements. Once accepted by eSafety, the undertaking can be enforced by a Court.
- **Injunctions**. An injunction is an order granted by a Court to compel an end-user or online service provider to take certain actions, or to refrain from taking certain actions, to comply with the Cyberbullying Scheme requirements.
- **Infringement notices**. Infringement notices are notices that set out the particulars of an alleged contravention and specifying an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings.
- **Civil penalty orders**. These are court orders that require a person who is found to have contravened a civil penalty provision of the Act to pay a penalty.

Review rights

Certain actions taken by eSafety under the Cyberbullying Scheme can be reviewed internally by eSafety and externally by the Administrative Review Tribunal[#]. The purpose of these review rights is to ensure that we have made the correct and preferable decisions on a case-by-case basis.

Under the Cyberbullying Scheme, a review can be requested when a removal notice or end-user notice has been given, or when eSafety has decided not to give a removal notice for material that meets the definition of cyberbullying.

Action which can be reviewed	Who can seek review?
Giving a removal notice	• The online service provider that received the notice • The end-user who posted, shared or sent the relevant material
Giving an end-user notice	• Generally, a person whose interests are affected by the notice
Refusing to give a removal notice	•The targeted child, or a responsible person with the targeted child's consent • The adult who made the complaint within 6 months after they reached 18 years of age about material targeting them when they were a child. • The person who made the complaint about the material to eSafety

Basic Online Safety Expectations

The Basic Online Safety Expectations (the Expectations) are a set of expectations set by the Australian Government for social media services, relevant electronic services and designated internet services. eSafety can require providers of these kinds of services to report on how they are meeting the Expectations.

The Basic Online Safety Expectations are focused on ensuring that these services take reasonable steps to keep Australian end-users safe including in relation to cyberbullying. They also aim to provide greater transparency and accountability around services' safety features, policies and practices. More information about the Expectations and how eSafety uses its powers to require transparency in relation to them can be found in the Basic Online Safety Expectations regulatory guidance on eSafety's website.

Find more information and support

For more information regarding cyberbullying, or to report cyberbullying to eSafety, please visit our website at eSafety.gov.au.

If you are in Australia and you are in immediate danger, call police on Triple Zero (000). If you are 25 or under and need support, you can call Kids Helpline anytime on 1800 55 1800. If you are 25 or over, please call Lifeline on 13 11 14.

[#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).

Published: January 2025 (Updated)

Online Safety Act 2021

Adult Cyber Abuse Scheme

Regulatory Guidance

eSC RG 3

Updated November 2025

Australian Government

eSafety Commissioner

eSafety.gov.au

Contents

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public, the online industry and other professionals who require further information about the Adult Cyber Abuse Scheme. It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to address adult cyber abuse. It also explains how eSafety will generally interpret and apply the law when responding to reports of adult cyber abuse.

All decisions made by eSafety will be made on a case-by-case basis, considering the particular circumstances of each matter.

Overview of the Adult Cyber Abuse Scheme

The Adult Cyber Abuse Scheme is a safety net to be used when a complaint has been made to an online service provider but the online service provider has not removed the material. The Adult Cyber Abuse Scheme has the following regulatory features:

1. **A system under which a person may make a complaint to eSafety** about adult cyber abuse material that targets an Australian who is 18 years or older. A complainant must have first reported the abuse to the relevant online service provider before eSafety can give a notice requiring removal of adult cyber abuse material.
2. **Investigative and information gathering powers** which allow eSafety to assess complaints of adult cyber abuse and decide what action we can take.
3. **Removal powers** which allow eSafety to give notices to online service providers, and to people (end-users) who have posted, shared or sent adult cyber abuse material, requiring them to remove the material. eSafety's removal powers only come into effect if a complaint has been made directly to an online service provider and they have failed to remove the material.
4. **Enforcement options** which are available to eSafety where there has been a failure to comply with our notices. These range from issuing a formal warning to seeking civil penalties.

Key terms

What is 'adult cyber abuse'?

Adult cyber abuse means online communication to or about a person who is 18 years or older which is intended to cause them serious harm. It must be communicated through a social media service, relevant electronic service or designated internet service. It can include posts, comments, emails, messages, memes, images and videos.

The Act[1] defines adult cyber abuse as material targeting a particular Australian adult that is **both**:

1. intended to cause serious harm, and

2. menacing, harassing or offensive in all the circumstances.

If the material only meets one of the two criteria above (for example, if the post is offensive but is found to not be intended to cause serious harm), it will not be considered adult cyber abuse under the Act.

Under the Act, the term 'adult cyber abuse' is reserved for the most severely abusive material intended to cause serious psychological or physical harm. This would include material which sets out realistic threats, places people in real danger, is excessively malicious or is unrelenting. eSafety may consider material collectively when assessing its overall seriousness.

The scheme is not intended to regulate hurt feelings, purely reputational damage, bad online reviews, strong opinions or banter.

Who is meant by 'a particular Australian adult'?

For eSafety to be able to act on a complaint, the material must target a particular Australian adult. The Act defines an Australian adult as a person who is 18 years or older and is ordinarily resident in Australia. eSafety cannot use its powers under the Adult Cyber Abuse Scheme to help adults resident in other countries. Children are covered by a separate scheme, the eSafety's **Cyberbullying Scheme**.

A 'particular' Australian adult means one specific person, not a broad range or group of people. For example, racist abuse targeting a group rather than an individual, such as a post that says all people of a certain background 'should be wiped out' would not be adult cyber abuse for the purposes of this scheme because it is directed at a group rather than a specific person.

However, a post that uses an ethnic slur to describe a specific person may be considered adult cyber abuse if it meets the adult cyber abuse threshold. For example, 'You are a [insert ethnic slur] and you should have been killed with your ancestors' is an example of hate speech targeting a specific person that may meet the adult cyber abuse threshold.

[1]Section 7 of the Act.

What is 'serious harm' in the context of the Adult Cyber Abuse Scheme?

The Act defines 'serious harm' to mean serious physical harm or serious harm to a person's mental health, whether temporary or permanent.

This includes serious psychological harm and serious distress that goes beyond 'mere ordinary emotional reactions such as those of only distress, grief, fear or anger'.[2]

On its own, purely financial harm, defamatory material that causes purely reputational harm, or incidental harm experienced as part of social or community interaction is not enough to be considered 'serious harm'. For example, negative online reviews of a business or false statements about a person's criminal history or character will not meet the threshold. Serious harm in the context of adult cyber abuse is to be considered objectively. It is not enough that a person felt seriously harmed by the material but rather whether an ordinary reasonable person would likely conclude that the post was intended to cause serious harm.

How does eSafety determine 'serious harm' in the context of adult cyber abuse?

eSafety will consider each matter on a case-by-case basis. Given the broad range of material on the internet, we cannot identify a single set of factors that may be considered. However, generally eSafety will consider the occurrence and prominence of the following factors to guide our inquiries:

- Revealing personal information to deliberately make someone feel unsafe, which is known as 'doxing'
- Urging or encouraging violence against a person including actively inciting self-harm
- Threats of violence
- Posts designed to generate volumetric and 'pile-on' attacks from others
- Relevant history between the target and the end-user
- Behaviour which is clearly targeting a known vulnerability of the person targeted that exacerbates that vulnerability. This might occur, for example, where there is evidence that the person posting, sharing or sending the material is aware of the targeted person's mental health history and the material is intended to worsen the targeted person's wellbeing
- Mitigating factors such as the age of the end-user. This will not definitively rule out seeking removal action, however it is a factor to be taken into account in determining appropriate responses, and
- Online incitement of any of the above activities.

What is meant by 'mere ordinary emotional reactions'?

For eSafety to be able to give a removal notice, the material must likely be intended to cause serious harm. Ordinary emotional reactions to upsetting online material – such as anger, fear, grief or distress – are not enough on their own to meet the Act's threshold for adult cyber abuse.

[2]Section 5 of the Act contains this definition.

In the absence of other factors such as those set out under the heading **"How does eSafety determine 'serious harm' in the context of adult cyber abuse?"** the following material will in most cases result in an ordinary emotional reaction and not serious harm:

- Name calling and opinions (for example, 'You are an ugly cow')
- Character attacks (for example, 'You are a lying bigot')
- Claims of criminal conduct (for example, 'I know you are a scammer and a thief')

Likewise, if the material is only expressed as a hope, wish or opinion then it is less likely to meet the threshold for being intended to cause serious distress.

What does 'menacing, harassing or offensive' mean?

Under the Act, whether something is menacing, harassing or offensive will be considered in light of the particular circumstances of the matter.

For example, eSafety will consider whether a person has been targeted because of their cultural background, gender, sexual orientation, disability, mental health condition or family or domestic violence situation. eSafety may also consider the actions of the person being targeted, including whether they have also posted, shared or sent menacing, harassing or offensive material themselves, which has been reported to eSafety. For example, if a person makes a complaint that they have been harassed because they have been sent a large number of abusive messages, it will be less likely to be considered harassing if eSafety becomes aware of the complainant also sending abusive messages to the person they claim has been harassing them. eSafety may also consider anything that is relevant about the person who posted, shared or sent the material, such as their age.

Menacing or harassing

'Menacing' and 'harassing' do not have a specific legal meaning under the Act. Although it will depend on the circumstances of each matter, eSafety considers it likely that conduct that is threatening and/or repetitive will fall within these definitions.

Offensive

Under the Act, eSafety must consider a number of matters when assessing what is and is not offensive, including:

- the standards of morality, decency and propriety generally accepted by reasonable adults
- the literary, artistic or educational merit (if any) of the material, and
- the general character of the material (including whether it is of a medical, legal or scientific character).[3]

Although it will depend on all the circumstances, eSafety considers that material will likely be offensive when:

- it is calculated to, or likely to, cause significant anger, significant resentment, outrage, disgust, or hatred, and
- it does more than simply hurt or wound a person's feelings.

[3]Section 8 of the Act.

Freedom of speech

The Adult Cyber Abuse Scheme is not intended to stifle freedom of speech, including in the context of political comments, legitimate expression or robust debates online. However, environments that allow serious abuse to spread can actually reduce freedom of speech, because people who are targeted by abuse feel silenced and may stop participating online. This can have the greatest impact on marginalised groups.

The Act balances these important concepts in two main ways:

- The Act states that the implied right to freedom of political communication will be protected, and[4]
- The threshold for adult cyber abuse under the Act is sufficiently high to ensure legitimate expressions of opinion will not be included.

Material that does not meet the threshold

The threshold for adult cyber abuse has been set deliberately high to ensure it does not inappropriately stifle freedom of speech. The threshold is higher than the threshold for the Cyberbullying Scheme that protects Australian children because adults are expected to have greater resilience than children.

However, eSafety recognises that a broad range of online material and behaviour can be abusive and harmful even if it does not meet the legal threshold for adult cyber abuse. Every situation is unique and eSafety is committed to helping all Australians who seek our assistance with online harm. Where we find that material does not meet the threshold for adult cyber abuse, eSafety will still try to help the person who made the complaint by:

- providing tips and information for avoiding or minimising the impact of abusive material
- directing them to resources and other organisations or agencies that may be able to provide further support
- considering whether the material may have breached the terms of use of the online service provider and, if serious enough, informally requesting removal (even though the service is not obliged to take action).

Making a complaint to eSafety

Who can complain?

A complaint about adult cyber abuse may be reported by the person targeted by the abuse, or another person who is authorised to report it on their behalf. The complaint can be made to eSafety through the online form on our website.

[4]Section 233 of the Act.

Complaint made by an Australian adult

An Australian adult can make a complaint if they have a reason to believe that they are, or have been, the target of adult cyber abuse material.[5]

The material must be, or have been, provided on:

- a social media service
- a relevant electronic service such as an email service, chat service, instant messaging service or an online game where end-users play against each other, or
- a designated internet service such as a website or app.[6]

Complaint made on behalf of an Australian adult

A responsible person may make a complaint on behalf of an Australian adult if the person has reason to believe that the adult is, or has been, the target of adult cyber abuse material on one of the online services listed in the previous section.[7] The responsible person must be authorised by the adult to make the complaint.

When a complaint is made on behalf of someone else, eSafety will work with the person making the complaint and the target of the material (if required) to confirm that the person making the complaint is authorised to do so.

Making a complaint to online service providers first

Before eSafety can give a removal notice for adult cyber abuse material, the person making the complaint must show that they have already made a complaint about the material to the relevant online service provider.[8] We will ask for this evidence through our online reporting form. eSafety cannot give a removal notice until at least 24 hours have passed since the report was made to the relevant online service provider.[9]

Many online services provide links or other methods for users to report abuse and they can remove material without help from eSafety. **The eSafety Guide** has more information about how to report issues to commonly used online services.

If the relevant online service provider supplies a receipt, reference or report number as part of its business processes, we will usually need to know that number. In cases where receipts are not provided, we will need a screenshot of the report or some other proof that it was made.

Otherwise, a statutory declaration can be provided – this is a legal document that contains a written statement saying something is true, which has been witnessed by an authorised person.

[5]Section 36(1) of the Act. [6]Section 36(1) of the Act. [7]Section 36(2) of the Act. [8]Sections 36(3), 88(1)(c), 89(1)(c) and 90(1)(c) of the Act. [9]Sections 88(1)(d), 89(1)(d) and 90(1)(d) of the Act.

Investigation of adult cyber abuse material

Under the Act, eSafety is empowered to investigate complaints about adult cyber abuse.[10]

eSafety may ask for any information from relevant people, organisations and online service providers, and make any other enquiries that we think will help with our investigation of an adult cyber abuse complaint.[11] eSafety may also end an investigation at any point.[12]

eSafety's investigative powers are set out in Part 14 of the Act. These powers include the ability to compel a person to answer questions and/or produce documents or other information.[13] eSafety has additional information-gathering powers under Part 13 of the Act to obtain end-user identity and contact information from the provider of a social media service, relevant electronic service or designated internet service.[14]

Prioritising Complaints

Due to the number of adult cyber abuse complaints eSafety receives, certain complaints may be prioritised for action. Some of the factors taken into account when deciding how to prioritise complaints include:

- the urgency of the situation
- the extent and nature of the abuse
- whether the target of the abuse has themselves engaged in behaviour amounting to cyber-abuse
- any identified vulnerability or risk factors present in relation to the person being targeted.

Approaches to compliance and enforcement

When seeking to have adult cyber abuse material removed, eSafety may take informal or formal action.

Informal requests

eSafety will often approach online service providers informally to ask them to remove adult cyber abuse material in the first instance. We have found that this generally results in faster removal of material compared to formal action, which is a better outcome for the targeted person.

Formal actions

While eSafety will generally seek informal removal of material, we will not hesitate to use our formal powers when we consider it appropriate. This includes going directly to end-users or online service providers where appropriate.

For example, if an online service provider has a history of not responding to eSafety's informal removal requests or there are other factors that suggest the online service provider is unlikely to respond to an informal removal request, eSafety may decide to give a removal notice without first approaching the online service provider informally for removal.

[10]Section 37(1) of the Act. [11]Section 37(2) of the Act. [12]Section 37(5) of the Act. [13]Sections 197 to 205 of the Act. [14]Sections 193 to 196 of the Act.

eSafety is aware that some online service providers and end-users may prefer to receive a formal notice to qualify for certain protections set out under section 221 of the Act. If this is the case, eSafety's preference is that this be made clear in any response to an informal request so we can assess the appropriateness of formal action as quickly as possible.

Compliance and enforcement options

Under the Act, eSafety can consider a range of formal compliance and enforcement options when investigating adult cyber abuse material.

Outcome	**Formal action** - directed towards end-users	**Formal action** - directed towards online service providers
Put an online service provider on notice		Give one of the following **service provider notifications**: • a written notice informing an online service provider that material that meets the definition of adult cyber abuse is on its service • a statement informing an online service provider that material that meets the definition of adult cyber abuse and that breaches the service's own terms of use is, or was, on its service on two or more occasions over the past 12 months. In addition, eSafety may publish this statement on our website.
Require removal of content	Give a removal notice to an end-user requiring the end-user to take all reasonable steps to remove the material within 24 hours (or longer if allowed by eSafety). This can be given where eSafety has received a valid complaint and eSafety is satisfied a complaint has been made about the material to the relevant online service provider and removal has not occurred within 24 hours.	Give a removal notice to an online service provider requiring the online service provider to take all reasonable steps to remove the material on the service or take all reasonable steps to cease hosting the material within 24 hours (or longer if allowed by eSafety). This can be given where a valid complaint has been received by eSafety and eSafety is satisfied a complaint has been made about the material to the relevant online service provider and removal has not occurred within 24 hours.
Take enforcement action	Options for failing to comply with a removal notice: • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. Failure to comply with a Part 14 notice may also attract certain penalties.	Options for failing to comply with a removal notice: • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. Failure to comply with a Part 13 or Part 14 notice may also attract certain penalties.

Service provider notifications

What are service provider notifications?

Generally, a service provider notification informs the online service provider that eSafety is aware that material which meets the definition of adult cyber abuse is on its service.

A service provider notification may be given to the provider of a social media service, relevant electronic service or designated internet service.[15]

When can eSafety give a service provider notification under the Adult Cyber Abuse Scheme?

Service provider notifications can be given to platforms in two circumstances:

- eSafety may give a written notice to an online service provider to make it aware of adult cyber abuse material targeting a particular Australian on its service following a complaint. We can give this notice to an online service provider even if a complainant has not yet made a complaint about the matter to the online service provider. This is a quick way of putting the online service provider 'on notice' about the adult cyber abuse material, and eSafety expects the notice would prompt the service provider to remove the material. eSafety may use this option where, for example, a less formal approach is likely to result in faster removal of material. This type of service provider notification can only be given with the consent of the complainant and does not give rise to enforcement options if the online service provider does nothing in response.[16]
- If adult cyber abuse material is, or was, available on the service on two or more occasions in the last 12 months, eSafety may:
  - prepare a statement to that effect,
  - publish the statement on our website, and
  - give a copy of the statement to the online service provider.

To give this statement, the material must also have breached the service's own terms of use. The purpose of publishing this statement is to call out services that are not doing enough to combat adult cyber abuse.[17] eSafety will generally give an online service provider a chance to comment (and take action) before determining whether to publish the statement.

What are the consequences of a service provider notification?

A service provider notification is a less formal approach than giving a removal notice and there is no enforcement action which arises from a failure to act after receiving such a notification.

However, eSafety expects that an online service provider would take action to remove the material without the need for eSafety to give a removal notice.

In addition, eSafety will consider a relevant online service provider's response to any notifications when considering other regulatory options.

[15]Section 93(1) of the Act. [16]Section 93(1) of the Act. [17]Section 93(2) of the Act.

Removal notices

What is a removal notice?

A removal notice is a written notice requiring the recipient to remove or take all reasonable steps to cease hosting adult cyber abuse material from a service within 24 hours or a longer timeframe as specified by eSafety.

A removal notice may be given to the relevant end-user[18] or to the provider of a social media service, relevant electronic service, designated internet service[19] or hosting service.[20]

Failure to comply with the notice enables eSafety to take a range of enforcement actions, from issuing a formal warning to seeking civil penalty orders.

When can eSafety issue a removal notice under the Adult Cyber Abuse Scheme?

eSafety may give a removal notice to a social media service, relevant electronic service or designated internet service provider where:

- eSafety has received a complaint about adult cyber abuse material
- the adult cyber abuse material has been provided on a social media service, relevant electronic service, designated internet service
- the adult cyber abuse material was the subject of a complaint made to the provider of the service
- the material was not removed from the service within 24 hours after the complaint was made or such longer period as eSafety allows
- eSafety is satisfied that the material is or was adult cyber abuse material targeted at an Australian, and
- the material can be identified in a way that enables the online service provider or end-user to comply with the notice such as for example through screenshots, URLs, usernames or time stamps.[21]

A removal notice can also be given to a hosting service provider where the material provided on a social media service, relevant electronic service or designated internet service is hosted by a hosting service provider and the criteria listed in this section are met.[22]

The Act does not impose any time limits within which a removal notice must be given.

The giving of a removal notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether action will be taken.

What are the consequences of a removal notice?

A person must comply with a requirement under a removal notice to the extent that the person is capable of doing so.[23]

Where a person fails to comply with a removal notice, they can face a civil penalty of up to 500 penalty units.[24] eSafety may also consider several other enforcement options.

[18]Section 89 of the Act. [19]Section 88 of the Act. [20]Section 90 of the Act. [21]Section 88, 89 and 90 of the Act. [22]Section 90 of the Act. [23]Section 91 of the Act. [24]The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against individual.

Taking enforcement action

Sometimes, eSafety needs to go a step further and take enforcement action against an end-user or online service provider who has failed to comply with a removal notice.

eSafety is empowered under the Act to address adult cyber abuse material through a range of actions. Where appropriate, eSafety takes a graduated approach to enforcement action.

Enforcement options available include the following:

- **Formal warnings.** A formal warning can be issued to advise an online service provider or end-user that they have failed to comply with the requirements of a removal notice, and they could face further consequences if they continue to fail to comply.
- **Enforceable undertakings**. An enforceable undertaking requires an online service provider to enter into an agreement with eSafety to ensure compliance with the Adult Cyber Abuse Scheme requirements. Once accepted by eSafety, the undertaking can be enforced by a Court.
- **Injunctions**. An injunction is an order granted by a Court to compel an end-user or online service provider to take certain actions, or to refrain from taking certain actions, to comply with the Adult Cyber Abuse Scheme requirements.
- **Infringement notices.** Infringement notices are notices that set out the particulars of an alleged contravention and specify an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings.
- **Civil penalty orders.** These are court orders that require a person who is found to have contravened a civil penalty provision of the Act to pay a penalty.

Review rights

Certain actions taken by eSafety under the Adult Cyber Abuse Scheme can be reviewed internally by eSafety and externally by the Administrative Review Tribunal[#]. The purpose of these review rights is to ensure that eSafety has made the correct and preferable decisions on a case-by-case basis.

Under the Adult Cyber Abuse Scheme, a review can be requested when a removal notice has been given, or when eSafety has decided not to give a removal notice for material that meets the definition of adult cyber abuse.

Action which can be reviewed	Who can seek review?
Giving a removal notice (online service provider)	• The online service provider that received the notice • The end-user who posted, shared or sent the relevant material
Giving a removal notice (end-user)	• Generally, a person whose interests are affected by the notice
Refusing to give a removal notice (online service provider)	• The targeted adult, or with the targeted adult's consent • The person who made the complaint about the material to eSafety

Basic Online Safety Expectations

The Basic Online Safety Expectations (the Expectations) are a set of expectations set by the Australian Government for social media services, relevant electronic services and designated internet services. eSafety can require providers of these kinds of services to report on how they are meeting the Expectations.

The Expectations are focused on ensuring that these services take reasonable steps to keep Australian end-users safe including in relation to adult cyber abuse. They also aim to provide greater transparency and accountability around services' safety features, policies and practices. More information about the Expectations and how eSafety uses its powers to require transparency in relation to them can be found in the Basic Online Safety Expectations regulatory guidance on **eSafety's website**.

Find more information and support

For more information regarding adult cyber abuse, or to report adult cyber abuse material to eSafety, please visit the website at **eSafety.gov.au**.

If you are in Australia and you are in immediate danger, call police on Triple Zero (000). If you are 25 or under and need support, you can call Kids Helpline anytime on 1800 55 1800. If you are 25 or over, please call Lifeline on 13 11 14.

[#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).

Published: November 2025 (Updated)

Online Safety Act 2021

Image-Based Abuse Scheme

Regulatory Guidance

eSC RG 2

Updated November 2025

Australian Government | eSafetyCommissioner

Contents

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public, the online industry and other professionals who require further information about the Image-Based Abuse Scheme. It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to address image-based abuse. It also explains how eSafety will generally interpret and apply the law when responding to reports of image-based abuse.

All decisions made by eSafety will be made on a case-by-case basis, considering the particular circumstances of each matter.

Overview of the Image-Based Abuse Scheme

The Image-Based Abuse Scheme provides eSafety with regulatory powers to remove and take action against the non-consensual sharing of, or threat to share, an intimate image online. The Image-Based Abuse Scheme consists of the following regulatory features under the Act:

1. **General prohibition on image-based abuse** allows eSafety to take action against a person (end-user) who shares online (or threatens to share) an intimate image without the consent of the person shown. An 'intimate image' can include a video.

2. **A system under which a person may make a complaint to eSafety** about image-based abuse online.

3. **A system under which a person may object** to an intimate image remaining online even if the person depicted originally consented to the intimate image being shared.

4. **Investigative and information gathering powers** which allow eSafety to assess complaints about image-based abuse and decide what action we can take.

5. **Removal powers** which allow eSafety to give notices to online service providers and end-users requiring them to remove an intimate image.

6. **Remedial direction** powers which allow eSafety to require an end-user, who has breached the general prohibition on image-based abuse, to take actions specified by eSafety to reduce the risk of further breaches (such as removing the images online and deleting images from their devices).

7. **Enforcement action** available to eSafety where there has been a breach of the general prohibition or a failure to comply with eSafety notices or directions. These range from issuing a formal warning to seeking civil penalties in court.

Key terms

What is 'image-based abuse'?

Image-based abuse means sharing online, or threatening to share, an **intimate image** without the consent of the person shown.

Image-based abuse is generally intended to cause harm, distress, humiliation and embarrassment. This can be through making the images or videos visible to particular people or the general public using an online service, or by threatening to make them visible (often in an attempt to control, coerce, 'punish' or blackmail the person targeted by the image-based abuse).

For eSafety to investigate a complaint about image-based abuse, the abuse must have happened on a social media service, relevant electronic service or a designated internet service. In addition, either the end-user who shared (or threatened to share) the image, or the person shown in the image, must be ordinarily resident in Australia.[1]

What is 'consent'?

To consent is to give permission for something to happen. This consent must be 'express, voluntary and informed',[2] which means that the person understands what they are being asked and has not been tricked or forced into agreeing to their intimate image being shared.

Legally, a person under the age of 18 cannot consent to their intimate image being shared, nor can a person who is in a mental or physical condition where they are not capable of giving consent or their capacity to consent is substantially impaired. It is against the law to share an intimate image of someone who is under the age of 18 or of someone who cannot give express, voluntary and informed consent even if that person has said that they agree.[3]

What does 'ordinarily resident in Australia' mean?

A person who is 'ordinarily resident in Australia' means a person who usually lives in Australia, even if they are overseas at the time of the alleged image-based abuse.

[1]Section 75(1) of the Act. [2]Section 21 of the Act. [3]Section 21 of the Act.

What is an 'intimate image'?

The Act[4] defines an 'intimate image' to be a still visual image or moving visual images that shows, or appears to show:

- a person's genital area or anal area (whether bare or covered by underwear);
- a person's breasts (if the person identifies as female, transgender or intersex);
- private activity (for example, a person in a state of undress, using the bathroom, showering, bathing or engaged in sexual activity)
- a person without attire of religious or cultural significance if they would normally wear such attire in public.

In addition, for an image or video to be considered 'intimate' it must also show the person in circumstances in which an ordinary reasonable person would 'reasonably expect to be afforded privacy'.

Intimate images can include photos and videos that have been digitally altered (for example, photoshopped images or deepfakes). They also include images or videos which have been shared in a way that will make people think they show a specific person (for example, a nude photo tagged with a person's name even though it is not of them). A blurred image or video may be an intimate image, taking into account all the circumstances and characteristics of the image. Intimate images would not usually include drawn images and graphic representations of a person, such as comics and cartoons.

What does 'without attire of religious or culture significance' mean?

Images or videos are considered to be intimate images if they show a person without clothing or accessories of religious or cultural significance that they consistently wear in public, in circumstances where the person would reasonably expect to be afforded privacy.

This is intended to recognise that an image of a person without particular religious or cultural attire that they consistently wear can cause significant harm to them. For example, a Muslim woman who consistently wears a niqab while in public or a Sikh man who consistently wears a turban in public.

What does 'reasonably expect to be afforded privacy' mean?

In simple terms, this means the intimate image must show a person at a time when they would have assumed they had privacy.

Whether there is a reasonable expectation of privacy depends on the circumstances of the image itself and its creation. Factors eSafety might consider include the extent of control the person shown has over who is permitted to see the intimate image and in what circumstances.

[4]Section 15 of the Act.

eSafety will also consider the surrounding circumstances of the creation of the intimate image, including the existence of a relationship of trust or whether there was an agreement or understanding governing the use of the image.

The notion of whether a person is shown in circumstances in which an 'ordinary reasonable person would reasonably expect to be afforded privacy' will generally be interpreted broadly. However, there are limits on when a person would expect to be afforded privacy under the Act. For example, eSafety is unlikely to take action where a person has deliberately made their image available online with no way of controlling its distribution.

Other examples of where it would be unlikely that there was an expectation of privacy under the Act include:

- an image of an underwear model taken in the course of that person's work where the image was created and used for a public advertising campaign or public art display
- an image of a topless bather at a public beach (as opposed to a private beach).

When a person consents to the sharing of an image or video, they may still have a reasonable expectation of (or entitlement to) privacy if their consent is limited to certain circumstances.

What is an 'exempt provision of an intimate image'?

eSafety cannot give a removal notice or take other enforcement action in relation to sharing of an image or video if the sharing took place in an exempt situation, even if the image or video meets the definition of an intimate image.[5]

Sharing an intimate image is exempt in the following situations:

- Where it is necessary for, or of assistance in:
  - enforcing a law, or
  - monitoring compliance with, or investigating a contravention of, a law.
- Where it is necessary for the purposes of proceedings in a court or tribunal.
- Where it is for a genuine medical or scientific purpose.
- Where an ordinary reasonable person would consider the shared post acceptable.[6]
- Where the person who posted the image is a 'protected person' (such as a member of staff of eSafety or the Australian Communications and Media Authority, or a member of the Classification Board).[7]
- Where the post was related to eSafety's exercise of its powers or functions.

[5]Section 86 of the Act. [6]Section 86(1)(g) of the Act sets out the criteria for this exemption. [7]Section 223 of the Act.

General prohibition

The posting or threatened posting of an intimate image to a social media service, a relevant electronic service or a designated internet service without the consent of the person shown is prohibited under the Act.[8] It is a civil penalty provision which is punishable by up to 500 penalty units.[9]

The general prohibition does not apply if the sharing of the intimate image is or would be exempt.[10]

For eSafety to consider action under this general prohibition, the person who is shown in the image must be ordinarily resident in Australia, or the end-user responsible for the sharing (or threatened sharing) of the intimate image must be ordinarily resident in Australia.

Actions that can be taken against an end-user who posts or threatens to post an intimate image in these circumstances include civil penalty proceedings, infringement notices, injunctions, enforceable undertakings and formal warnings. eSafety is empowered to consider any enforcement option regardless of whether or not a removal notice has been given to the end-user.

Intimate images which show a person without attire of religious or culture significance

The general prohibition on image-based abuse does not apply to intimate images if the end-user who shared them did not know that the person shown normally wears attire of religious or cultural significance when in public. In these circumstances a remedial direction (such as a direction to delete a photo) cannot be made by eSafety, as this power can only be used when there is a breach of the general prohibition.

This exception is required in the Act because, unlike the other types of intimate images, what is considered intimate by the person shown depends on the religious or cultural practices of that person and their community, not on general interpretation. Anyone who wishes to rely on the exception must be able to provide evidence establishing that they did not know that the person shown normally wears religious or cultural attire in public.

This exception is designed to limit the liability of end-users who did not know about the intimate nature of the image or video they shared, but it does not prevent eSafety from helping the person shown without their religious or cultural attire. eSafety can still assess the image or video as intimate and give a removal notice in these circumstances.[11]

[8]Sections 75(1) and 75(2) of the Act. [9]The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against individual. [10]Section 75(4) of the Act. [11]Section 75(3) of the Act.

Making a complaint to eSafety

Who can complain?

A complaint about image-based abuse can be made to eSafety when both these conditions have been met:

- a person has reason to believe their intimate image has been shared (or a threat has been made to share it) on a social media service, a relevant electronic service or a designated internet service without their consent
- the person shown in the intimate image is ordinarily resident in Australia or the end-user accused of sharing (or threatening to share) the intimate image is ordinarily resident in Australia.[12]

A person making a complaint about image-based abuse does not need to have reported the image or video to the online service provider where it appeared before making a complaint to eSafety. A person can still make a complaint even if they cannot identify the end-user who shared the intimate image.[13]

The complaint can be made to eSafety through the online form on **our website**.

Once a complaint is received, eSafety is empowered to consider compliance and enforcement actions.

Making a complaint on behalf of someone else

A person can make a complaint on behalf of another person whose intimate image has been shared (or where there are threats to share that person's intimate image) if they are:

- authorised by the person shown in the intimate image,[14] or
- the parent or guardian of a child less than 16 years of age who is shown in the intimate image,[15] or
- the parent or guardian of the person shown in the intimate image and the person shown has a mental or physical condition (whether temporary or permanent) that makes them incapable of managing their affairs.[16]

When a complaint is made on behalf of someone else, eSafety will need a declaration confirming that person is authorised to make the complaint.[17] eSafety will work with the person making the complaint and the person shown in the image or video to confirm that the person making the complaint is authorised to do so.

[12]Section 32 of the Act. [13]Section 32(2) of the Act. [14]Section 32(3)(a) of the Act. [15]Section 32(3)(b) of the Act. [16]Section 32(3)(c) of the Act. [17]Section 32(4) of the Act.

Giving eSafety an objection notice

Who can give an objection notice?

Even when a person has previously given consent to share their intimate image they may later object to its continued availability. This objection notice can be given to eSafety through the online form on our website.

Objection given by the person shown in the intimate image

An objection notice can be given to eSafety when a person has reason to believe that their intimate image has been posted on a social media service, a relevant electronic service or a designated internet service.

In addition, any one of the following conditions must be met:

- the person who is shown in the intimate image is ordinarily resident in Australia
- the end-user responsible for posting the intimate image is ordinarily resident in Australia
- the intimate image is hosted in Australia.

eSafety will then be empowered to consider whether to give a removal notice. The decision will also depend on whether the sharing of the intimate image is exempt.

Objection given on behalf of someone else

An objection notice can be given to eSafety on behalf of another person, if the person who gives the objection to eSafety is:

- authorised by the person shown in the intimate image, or
- the parent or guardian of a child less than 16 years of age who is shown in the intimate image, or
- the parent or guardian of person shown in the intimate image, and the person shown has a mental or physical condition (whether temporary or permanent) that makes them incapable of managing their affairs.[18]

When an objection notice is given on behalf of someone else, eSafety will need a declaration confirming that person is authorised to give the objection notice. eSafety will work with the person giving the objection notice and the person shown in the image to confirm that the person giving the objection notice is authorised to do so.

An objection notice can be given even if the person shown in the intimate image consented to it being shared online.[19]

[18]Section 33(3) of the Act. [19]Section 33(5) of the Act.

Investigation of image-based abuse

eSafety is empowered to investigate complaints of image-based abuse under the Act.[20]

Under the Act, eSafety may obtain information from such persons, and make such inquiries, as we think will help with our investigation of an image-based abuse complaint.[21] eSafety may also end an investigation at any point.[22]

eSafety's investigative powers are set out in Part 14 of the Act. These powers include the ability to compel a person to answer questions and/or produce documents or other information.[23] eSafety has additional information-gathering powers under Part 13 of the Act to obtain end-user identity and contact information from a social media service, relevant electronic service or designated internet service.[24]

Prioritising Complaints

Due to the volume of image-based abuse complaints eSafety receives, we prioritise complaints that require the quickest compliance and enforcement action. As part of this process, we take into account a number of factors, including:

- the urgency of the situation
- the extent and nature of the abuse
- whether the image is currently online and the accessibility of the image
- any vulnerability or risk factors experienced by the person being targeted
- whether the intimate image was created for a commercial purpose.

If the complaint is against an unknown end-user who is threatening to share an intimate image without consent unless their demands are met, that is a type of blackmail called sexual extortion.

Reports of adult sexual extortion involving threats to share intimate images for financial demands

Safety receives a high volume of reports involving adult sexual extortion, where individuals are threatened with the sharing of intimate images or videos of them unless a financial demand is paid. These threats are often part of scams that trick people into sharing intimate content or engaging in sexual activity online. The scams frequently involve offshore perpetrators and encrypted messaging platforms. The image may not be shared publicly if the victim does not pay. The image may be shared publicly even if the victim does pay.

Due to the nature and volume of these reports, eSafety may not be able to take direct enforcement action. However, we remain committed to supporting Australians affected by this conduct. Each report is recorded in our system and manually reviewed by an eSafety investigator. This review helps us assess whether further action can be taken in line with our Compliance and Enforcement Policy, including determining whether the report meets criteria for potential enforcement or additional support. Where appropriate, reports may be further investigated. Individuals who submit a report will receive an automated email response containing information about sexual extortion and links to self-help resources. They are advised that further

[20]Section 34(1) of the Act. [21]Section 34(3) of the Act. [22]Section 34(5) of the Act. [23]Sections 197 to 205 of the Act. [24]Sections 193 to 196 of the Act.

communication from eSafety is unlikely to occur unless manual review identifies that additional support or enforcement action is possible. However, they are encouraged to provide any new information of relevance via email, so it can be considered during, or after, the manual review.

For example, this could include evidence that the intimate image or video has been posted online, evidence of any reasons to believe the blackmailer usually lives in Australia, or evidence that the demands are not (or not only) for financial payment.

Images created for a commercial purpose

eSafety is unlikely to prioritise matters where an image was originally created for a commercial purpose. The Image-Based Abuse Scheme is not intended to capture commercial breaches where there has been a breach of copyright.

In most cases, eSafety will not take any enforcement action in relation to image-based abuse complaints relating to an intimate image created for a commercial purpose. However, eSafety recognises that harm can occur in relation to these images which may require appropriate action. We determine the priority of matters requiring compliance and enforcement action on a case-by-case basis. Relevant factors include:

- whether the person has attempted to remove all of the relevant intimate images, including from the sites where they were originally monetised
- whether the person is still posting intimate images for commercial reasons
- whether the intimate images were originally available only to a limited subscriber base
- where continued availability of the intimate images will cause the person significant harm or distress.

Approaches to compliance and enforcement

Under the Act, eSafety can consider a range of formal compliance and enforcement options when investigating image-based abuse and, where appropriate, may consider making informal requests as well.

Informal requests

In the first instance, eSafety typically approaches online service providers to ask them to remove an intimate image, or to alert them to an account which is being misused to threaten to post an intimate image. We find that this generally results in faster removal of material compared to formal action, which is a better outcome for the person shown in the image. This is also preferable for online service providers, particularly where they are committed to resolving the complaints we raise with them swiftly and amicably.

Formal actions

While we prefer to seek rapid voluntary removal of material by online service providers, we do use our formal powers when we consider it appropriate.

For example, if an online service provider has a history of not responding to our informal requests or there are other factors that suggest the online service provider is unlikely to respond to an informal removal request, we may decide to issue a removal notice without first approaching them informally for removal.

Compliance and enforcement options

Under the Act, eSafety can consider a range of formal compliance and enforcement options when investigating image-based abuse.

Outcome	**Formal action** - end-user	**Formal action** - online service provider
Put an online service provider on notice		Issue one of the following **service provider notifications**: • a written notice informing an online service provider that an intimate image has been shared without consent on its service • a written statement informing an online service provider that an intimate image of a person shared without their consent, which breaches the service's own terms of use, is or was on their service on two or more occasions over the past 12 months. In addition, eSafety may publish this statement on our website. **See full details below of the circumstances when these notifications can be provided.**
Require removal of content	Give a **removal notice** requiring the end-user to take all reasonable steps to remove the material within 24 hours (or a longer timeframe specified by eSafety) arising from one of the following: • a complaint • an objection notice.	Give a **removal notice** requiring the online service provider to take all reasonable steps to remove the material within 24 hours (or a longer timeframe specified by eSafety) arising from one of the following: • a complaint • an objection notice.
	Give a **remedial direction** arising from the breach of the general prohibition not to share, or threaten to share, intimate images without the consent of the person shown.	
Take enforcement action	Options for breaching the general prohibition or failing to comply with a removal notice or remedial direction: • issue a formal warning • accept an enforceable undertaking • seek a court injunction • issue an infringement notice • seek a civil penalty order. Failure to comply with a notice given under Part 14 of the Act[25] may also attract certain penalties.	Options for failing to comply with a removal notice • issuing a formal warning • accept an enforceable undertaking • seek a court injunction • issue an infringement notice • seek a civil penalty order. Failure to comply with a notice given under Part 13 or Part 14 of the Act[26] may also attract certain penalties.

[25]Part 14 Notice refers to a notice given under the investigative powers outlined in Part 14 of the Act. [26]Part 13 Notice refers to a notice given under the information-gathering powers outlined in Part 13 of the Act. Part 14 Notice refers to a notice given under the investigative powers outlined in Part 14 of the Act.

Service provider notifications

What are service provider notifications?

Generally, a service provider notification informs the online service provider that eSafety is aware that material which meets the definition of an intimate image is on its service and eSafety has received a complaint or objection notice about the intimate image.

A service provider notification may be given to the provider of a social media service, relevant electronic service or designated internet service.[27]

When can eSafety give a service provide notification under the Image-Based Abuse Scheme?

A service provider notification can be given to an online service in two circumstances:

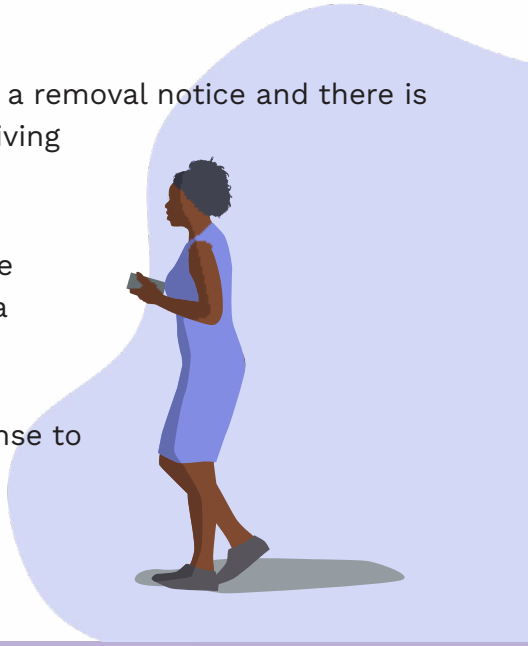
- A written notice may be used by eSafety to make an online service provider aware of an intimate image on its service following a complaint or an objection notice. This is a quick way of putting the service provider 'on notice' about an intimate image on their service, and eSafety expects the notice would prompt the service provider to remove the material. eSafety may use this option where, for example, a less formal approach is likely to result in faster content removal. The written notice will identify the image and state that eSafety is satisfied the person depicted did not consent to the provision of the image on the service. This type of service provider notification can only be given with the consent of the complainant and does not give rise to enforcement options if the online service provider does nothing in response.[28]
- eSafety may provide a statement to an online service provider where an intimate image of a person is, or was, available on the service on two or more occasions over the past 12 months. To give this statement, the material must also have breached the service's own terms of use and the person shown in each intimate image must not have consented to the intimate image being provided on the service. eSafety may also publish this statement on its website. The purpose of publishing this statement is to call out a service if it is not doing enough to combat image-based abuse.[29] eSafety will generally give an online service provider an opportunity to comment (and take action) before determining whether to exercise its discretion to publish such a statement.

What are the consequences of a service provider notification?

A service provider notification is a less formal approach than giving a removal notice and there is no enforcement action which arises from a failure to act after receiving such a notification.

However, eSafety expects that an online service provider would take action to remove the content without the need for eSafety to give a removal notice.

In addition, eSafety will consider an online service provider's response to any notification when considering other regulatory options.



[27]Section 85 of the Act. [28]Section 85(1) of the Act. [29]Section 85(2) of the Act

Removal notices

What is a removal notice?

A removal notice is a written notice requiring the recipient to take all reasonable steps to remove, or to take all reasonable steps to cease hosting, an intimate image on a service within 24 hours (or a longer timeframe specified by eSafety).

A removal notice may be given to the relevant end-user[30] or to the provider of a social media service, relevant electronic service, designated internet service[31] or hosting service.[32]

Failure to comply with the notice enables eSafety to take a range of enforcement actions, from issuing a formal warning to seeking civil penalty orders.

When can eSafety give a removal notice under the Image-Based Abuse Scheme?

eSafety may give a removal notice if all the following criteria are met:

- An intimate image (as defined by the Act) has been provided on a social media service, a relevant electronic service or a designated internet service.
- The intimate image is the subject of a valid complaint (and eSafety is satisfied that the person shown did not consent to it being shared online) or an objection notice (regardless of whether the person shown consented or not).
- The sharing of the intimate image did not place in an exempt situation.
- The material can be identified in a way that enables the online service provider or the end-user to comply with the notice (for example through screenshots, URLs, usernames or time stamps).[33]

A removal notice can also be given to a hosting service where the material provided on a social media service, relevant electronic or designated internet service is hosted by a hosting service provider and the criteria listed in this section are met.[34]

The Act does not impose any time limits within which a removal notice must be given.

The giving of a removal notice is ultimately at eSafety's discretion. This means eSafety makes the final decision about whether compliance action will be taken.

What are the consequences of a removal notice?

A person must comply with a requirement under a removal notice to the extent that the person is capable of doing so.[35]

Failure to comply with a removal notice may result in a civil penalty of up to 500 penalty units.[36] eSafety may also consider several other enforcement options.

[30]Section 78 of the Act. [31]Section 77 of the Act. [32]Section 79 of the Act. [33]Section 77, 78 and 79 of the Act. [34]Section 79 of the Act. [35]Section 80 of the Act. [36]The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against individual.

Remedial directions

What is a remedial direction?

A remedial direction is a written communication that requires the recipient to take specific action aimed at preventing, or preventing further, sharing of intimate images without consent.

Generally, a remedial direction will be best suited to matters where a warning and/or removal notice is insufficient to address the risk of future abuse. For example, if an end-user has threatened to post an intimate image, eSafety may direct the end-user not to do so and to delete the image from their device.

When can a remedial direction be given?

eSafety may give a remedial direction to an end-user who has contravened the general prohibition of image-based abuse under section 75 of the Act, regardless of whether a removal notice has already been given to them or to an online service provider.

A remedial direction cannot be given if the intimate image shows someone without cultural or religious attire and the end-user who posted it did not know that the person shown normally wears that attire in public.[37]

A remedial direction also can't be given if the person depicted had previously consented to the posting of the intimate image.[38]

A remedial direction may be used in conjunction with, or as an alternative to, other compliance and enforcement action.

The Act does not impose any time limit within which a remedial direction must be given following the image-based abuse. In addition, the Act does not specify the time limit within which an end-user must comply with a remedial direction – this is set by eSafety.

What are the consequences of a failure to comply with a remedial direction?

A person must not contravene a remedial direction.[39]

Contravention of a remedial direction may result in a civil penalty of up to 500 penalty units.[40] eSafety may also consider other enforcement options.

[37]Section 75(3) of the Act. [38]s75(2) of the Act. [39]Section 83(3) of the Act. [40]The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against individual.

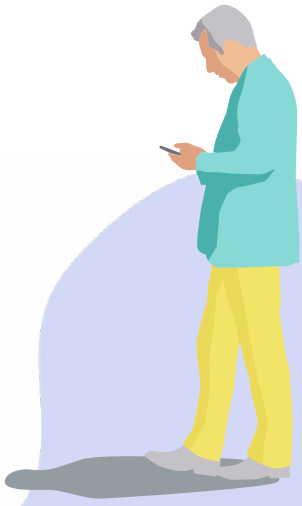
Taking enforcement action

Sometimes eSafety needs to go a step further, taking enforcement action against an end-user who has failed to comply with the general prohibition, a remedial direction or a removal notice, or an online service provider who has failed to comply with a removal notice.

eSafety is empowered under the Act to address image-based abuse through a range of actions. Where appropriate, eSafety takes a graduated approach to enforcement action.

Enforcement options available include the following:

- **Formal warnings**. A formal warning can be issued to either an online service provider[41] or an end-user[42] to advise them that they have breached a civil penalty provision under the Image-Based Abuse Scheme.
- **Enforceable undertakings.** An enforceable undertaking requires an end-user or an online service provider to enter into an agreement with eSafety to ensure compliance with the Image-Based Abuse Scheme requirements. Once accepted by eSafety, the undertaking can be enforced by a Court.
- **Injunctions.** An injunction is an order granted by a Court to compel an end-user or online service provider to take certain actions, or to refrain from taking certain actions, to comply with the Image-Based Abuse Scheme requirements.
- **Infringement notices.** Infringement notices are notices that set out the particulars of an alleged contravention and specify an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings.
- **Civil penalty orders.** These are court orders that require a person who is found to have contravened a civil penalty provision of the Act to pay a penalty.



[41]The civil penalty provision under the Image-Based Abuse Scheme for an online service provider is failing to comply with a removal notice (section 80 of the Act). [42]The civil penalty provisions under the Image-Based Abuse Scheme for an end-user are breaching the general prohibition (section 75 of the Act), failing to comply with a removal notice (section 80 of the Act) and failing to comply with a remedial direction (section 83 of the Act).

Review rights

Certain actions taken by eSafety under the Image-Based Abuse Scheme can be reviewed internally by eSafety and externally by the Administrative Review Tribunal[#]. The purpose of these review rights is to ensure that we have made a correct and preferable decision in each case.

A review can be requested when a removal notice or remedial direction has been given, or when eSafety has decided not to give a removal notice to an online service provider for material that was the subject of a valid complaint and was not exempt for any reason.

Action which can be reviewed	Who can seek review?
Giving a removal notice (online service provider)	• The online service provider who received the notice • The end-user who posted the content to the service
Giving a removal notice (end-user)	• Generally, a person whose interests are affected by the decision
Giving a remedial direction	• Generally, a person whose interests are affected by the decision
Refusing to give a removal notice (online service provider)	• The person shown in the intimate image, or an authorised person with the depicted person's consent • The person who made the complaint about the intimate image to eSafety

Basic Online Safety Expectations

The Basic Online Safety Expectations (the Expectations) outline the Australian Government's expectations that social media, messaging and gaming service providers and other apps and websites will take reasonable steps to keep Australians safe online. The Expectations are designed to improve providers' safety standards and improve transparency and accountability.

Under the Act, eSafety can issue a statutory notice requiring a provider of these kinds of services to report on how they are meeting the Expectations and can publish a summary of the information provided.

The purpose of the Expectations is to encourage online service providers to take reasonable steps to keep Australian end-users safe online, including in relation to image-based abuse. More information about the Expectations and how eSafety uses its powers to require transparency in relation to them can be found in the Basic Online Safety Expectations Regulatory Guidance on **eSafety's website**.

Find more information and support

For more information regarding image-based abuse, or to make a report of image-based abuse to eSafety, please visit the website at **eSafety.gov.au**.

If you are in Australia and you are in immediate danger, call police on Triple Zero (000). If you are 25 or under and need support, you can call Kids Helpline anytime on 1800 55 1800. If you are 25 or over, please call Lifeline on 13 11 14.

[#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).

Updated November 2025

Document created pursuant to section 17 of the *Freedom of Information Act 1982* (Cth)

A summary of the number of complaints or reports received by the eSafety Commissioner during the period 1 January 2023 to 8 May 2026, including breakdowns by category of online harm (such as cyberbullying, image-based abuse, and harmful online content):

	2023	2024	2025	2026 (to 8 May)	Total
Adult Cyber Abuse	2,846	3,501	4,667	2,218	**13,232**
Cyberbullying	2,517	3,186	3,448	1,302	**10,453**
Image-based Abuse	9,629	6,672	7,569	3,535	**27,405**
Illegal and Restricted Content	12,632	17,037	24,827	8,814	**63,310**
Total	**27,624**	**30,396**	**40,511**	**15,869**	**114,400**

References to years are to calendar years.

A summary of the number of complaints or reports received by the eSafety Commissioner for the period 1 January 2023 to 8 May 2026 involving TikTok, YouTube and Instagram:

	INSTAGRAM	TIKTOK	YOUTUBE
Cyberbullying	**2,452**	**3,971**	**219**
2023	711	818	56
2024	815	1,091	64
2025	738	1,387	75
2026 (to 8 May)	188	675	24
Adult Cyber Abuse	**2,436**	**2,364**	**344**
2023	473	451	90
2024	668	452	94
2025	887	937	123
2026 (to 8 May)	408	524	37
Image-Based Abuse	**8,047**	**1,233**	**208**
2023	3,800	267	89
2024	1,689	323	71
2025	1,658	353	31
2026 (to 8 May)	900	290	17
Illegal & Restricted Content	**1,220**	**839**	**2,157**
2023	187	113	570
2024	349	136	491
2025	525	372	740
2026 (to 8 May)	159	218	356
Total	**14,155**	**8,407**	**2,928**

References to years are to calendar years.