Basic Online Safety Expectations

Regulatory Guidance

July 2022

Australian Government | eSafetyCommissioner

esafety.gov.au

Contents

Overview of this guidance

This guidance is for members of the general public, industry and other stakeholders who require information about the Basic Online Safety Expectations, also known as 'the Expectations'.

The 'Expectations' are a key part of the Online Safety Act 2021 (the Act), and focus on ensuring providers of social media services, messaging services, gaming services, file sharing services and other apps and certain other sites accessible from Australia, take reasonable steps to keep Australians safe online. The aim is to increase the transparency and accountability of online service providers, thereby helping to incentivise and improve safety standards.

This guidance provides information on:

- how providers should seek to implement the Expectations
- how eSafety intends to approach compliance and enforcement
- how providers can share basic information, such as contact details, with eSafety, as required by the Expectations
- how providers should respond to requests for information, notices or determinations from eSafety
- providers' review rights.

Overview of the Expectations

The Act provides for the Minister to set online safety expectations through a legislative instrument called a determination. The Online Safety (Basic Online Safety Expectations) Determination 2022 – referred to as 'the Determination' – was registered on 23 January 2022. An Explanatory Statement was also published.

While the Expectations are not enforceable, eSafety has a number of relevant powers under the Act:

- The power to require online service providers to report on how they are meeting any or all of the Expectations, either on a non-periodic or a periodic basis. The obligation to respond to a reporting notice is an enforceable obligation and backed by civil penalties.
- The power to require reporting can either apply to specific providers, or via a legislative instrument – a determination – may apply to a specified class of providers.
- The power to issue statements to provider(s) about compliance and non-compliance with the Expectations and publish such statements.

The Expectations include a range of foundational steps that providers are expected to take to ensure safety for their users, as summarised in the following table.

Table one: Summary of the Expectations

Division	Headline Expectation	Expectations	Examples of reasonable steps that could be taken (where provided in the Determination) or qualifications
2. Safe use[1]	(S 6) Reasonable steps to ensure safe use.	The provider of the service will take reasonable steps to ensure that end-users are able to use the service in a safe manner. The provider of the service will take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful.	**Examples of reasonable steps:** **(a)** Developing and implementing processes to detect, moderate, report and remove (as applicable) material or activity on the service that is unlawful or harmful. **(b)** Ensuring that the default privacy and safety settings of the children's service are robust and set to the most restrictive level - if a service or a component of a service (such as an online app or game) is targeted at, or being used by, children (the children's service). **(c)** Ensuring that persons who are engaged in providing the service, such as the provider's employees or contractors, are trained in, and are expected to implement and promote, online safety. **(d)** Continually improving technology and practices relating to the safety of end-users. **(e)** Ensuring that assessments of safety risks and impacts are undertaken, and safety review processes are implemented, throughout the design, development, deployment and post-deployment stages for the service.
	(S 7) Consult with the eSafety Commissioner and refer to the Commissioner's guidance in determining such reasonable steps to ensure safe use.	The provider will consult the Commissioner in determining the reasonable steps to ensure safe use. The provider will also have regard to any relevant guidance material made available by the Commissioner.	

[1]Division 1 provides an overview of the purpose of the Determination.

Division	Headline Expectation	Expectations	Examples of reasonable steps that could be taken (where provided in the Determination) or qualifications
2. Safe use	(S 8) Reasonable steps regarding encrypted services.	If the service uses encryption, the provider will take reasonable steps to develop and implement processes to detect and address material and activity on the service that is unlawful or harmful.	**Qualifications** This expectation does not create a requirement to: **1.** implement or build a systemic weakness, or systemic vulnerability, into an encrypted service **2.** build a new decryption capability into an encrypted service **3.** render methods of encryption less effective.
	(S 9) Reasonable steps regarding anonymous accounts.	If the service permits the use of anonymous accounts, the provider will take reasonable steps to prevent those accounts being used to deal with material, or for activity, that is unlawful or harmful.	**Examples of reasonable steps** **1.** Having processes that prevent the same person from repeatedly using anonymous accounts to post material, or engage in activity, that is unlawful or harmful. **2.** Having processes in place that require verification of identity or ownership of accounts.
	(S 10) Consult and cooperate with other services to promote safe use.	The provider will take all reasonable steps to consult and cooperate with other service providers to promote the ability of end-users to use all those services in a safe manner.	**Examples of reasonable steps** **1.** Working with other service providers to detect high volume, cross-platform attacks (also known as 'pile-on' or 'volumetric' attacks). **2.** Sharing information with other service providers about unlawful or harmful material and activity for the purpose preventing and dealing with such material or activity.
3. Certain material	(S 11) Reasonable steps to minimise provision of certain material.	The provider will take reasonable steps to minimise the extent to which the following material is provided on the service: **1.** Cyberbullying material targeted at an Australian child. **2.** Adult cyber abuse material. **3.** Non-consensual intimate images of a person. **4.** Class 1 material. **5.** Material promoting, inciting, instructing in or depicting abhorrent violent conduct.	
	(S 12) Reasonable steps to prevent access by children to class 2 material.	The provider will take reasonable steps to ensure that technological and other measures are in effect to prevent access by children to class 2 material provided on the service.	**Examples of reasonable steps** **1.** Implementing age assurance mechanisms. **2.** Conducting child safety risk assessments.

Division	Headline Expectation	Expectations	Examples of reasonable steps that could be taken (where provided in the Determination) or qualifications
4. Reports and complaints	(S 13) Mechanisms to report and make complaints about certain material.	The provider will ensure that the service has clear and readily identifiable mechanisms that enable end-users and any person ordinarily resident in Australia to report and make complaints about certain material provided on the service.	
	(S 14) Service has terms of use, policies, procedures to deal with complaints.	The provider will ensure that the service has: **1.** terms of use **2.** policies and procedures relating to end-user safety **3.** policies and procedures for dealing with complaints and reports **4.** standards of conduct for end-users **5.** policies and procedures relating to content moderation and the enforcement of conduct standards. Providers will take reasonable steps so that penalties for breaches of terms of use are enforced against all accounts held or created by the end-user who breached the terms of service.	
	(S 15) Service will have mechanisms to report and make complaints about breaches of terms of use.	The provider will ensure that the service has clear and readily identifiable mechanisms that enable: **1.** end-users, and **2.** any person ordinarily residing in Australia, to report, and make complaints about, breaches of the service's terms of use.	
	(S 16) Accessible information on how to complain to eSafety.	The provider will ensure that there is readily accessible information and guidance provided to end-users on how to make a complaint to eSafety, in accordance with the Online Safety Act 2021, about any of the 'certain material' listed above – including class 2 material.	
5. Accessible information	(S 17) Information on terms of use, policies and complaints made accessible.	The provider will provide information on: **1.** terms of use, policies and procedures, and standards of conduct **2.** online safety and parental control settings – including the availability of tools and resources published by eSafety. The provider will ensure that that this information is: **1.** readily accessible to end-users **2.** accessible at all points in the end-user experience (for online safety settings, parental controls, and eSafety resources) **3.** regularly reviewed and updated **4.** written in plain language.	
	(S 18) End-users receive updated information about changes to policies, terms and conditions, or similar documents.	The provider will ensure that end-users receive plain language updates about any changes to the information listed above. Such updates include targeted in-service communications.	
6. Record Keeping	(s19) Records of end-user-reports and complaints to be kept for five years.	The provider will keep records of reports and complaints about certain material provided on the service for five years after the report or complaint is made.	

Division	Headline Expectation	Expectations	Examples of reasonable steps that could be taken (where provided in the Determination) or qualifications
7. Dealings with the Commissioner	(S 20) Provider will provide requested information to the Commissioner.	The provider must comply within 30 days if the Commissioner gives them a written notice requesting: **1.** A statement that sets out the number of complaints made to the provider during a specified period (not shorter than six months) about breaches of the service's terms of use. **2.** A statement that sets out, for each removal notice given to the provider during a specific period (not shorter than six months), how long it took the provider to comply with the removal notice. **3.** Specified information relating to the measures taken by the provider to ensure that end-users are able to use the service in a safe manner. **4.** A report on the performance of online safety measures that the provider has announced publicly or reported to the Commissioner.	
	(S 21) Provider will have a designated contact point.	**1.** The provider will ensure that there is an employee, or agent of the provider, that is designated as the service's contact point for the purposes of the Online Safety Act 2021. **2.** The provider will ensure that this contact person's e-mail address and phone number are given to the Commissioner. **3.** If there is a change to the identity or contact details of the contact point, the provider will give the Commissioner written notice of the change within 14 days.	

Key terms

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

Class 1 material[2] is material 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.[3]

Class 2 material is material[4] that is, or would likely be, classified as either:

- X18+ (or, in the case of publications, category 2 restricted),[5] or
- R18+ (or, in the case of publications, category 1 restricted)[6] 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.

Additional information on the classification of material is available in the Online Content Scheme Regulatory Guidance on eSafety's website.

[2]Section 106 of the Act. This material includes films, publications, computer games and any other material that is not a film, publication or computer game.
[3]National Classification Code: https://www.legislation.gov.au/Details/F2013C00006.
[4]Section 107 of the Act. This material includes films, publications, computer games and any other material that is not a film, publication or computer game.
[5]Section 107(1)(a) - (e) of the Act.
[6]Section 107(1)(f) - (l) of the Act.

What is 'unlawful' material?

'Unlawful' is used in the Determination to refer to material or activity that is not permitted under a Commonwealth Act. For the purposes of the Determination, the term 'unlawful' refers to illegal material or activity dealt with under the Act and other unlawful material or activities that may have a negative impact on the online safety of Australians, such as incitement or instruction to commit crime.

What is 'harmful' material?

'Harmful' is used in the Determination to mean material or activity that is not unlawful, but is covered within the scope of the Act (for instance, class 2 material). It is also used to mean material or activity that falls under a service provider's terms of use, policies and procedures and standards of conduct for end-users (as outlined in Section 14 of the Determination).

Objectives for the Expectations

eSafety will focus on the following objectives when regulating implementation of the Expectations:

- Enhancing online service providers' transparency and accountability, and improving insights into the effectiveness and impact of what providers are doing to keep users safe online.
- Tracking harms, safety interventions and technology over time through use of periodic reporting notices and improving understanding of where gaps and challenges exist.
- Incentivising proactive and systemic safety interventions, including by using statements of compliance/non-compliance with the Expectations to highlight good practice, as well as areas where insufficient action is being taken.

eSafety's approach

eSafety expects that online service providers review their policies, procedures and practices to ensure alignment with the Expectations on a regular basis and that they develop plans to put in place additional measures where they are not compliant.

eSafety intends to take a phased approach to exercising powers related to the Expectations starting with the use of non-periodic notices with a focus on specific Expectations and acute issues of particularly high harm, such as child sexual exploitation and abuse. eSafety is able to use notices to require reporting from 24 July 2022, six months after the Determination was registered. More information can be found in the reporting powers section of this document.

eSafety is committed to the following principles when assessing providers' implementation of the Expectations:

- Applying eSafety's powers under Part Four of the Act in a fair and proportionate way, based on evidence and insights, and focusing on Australia-specific information.
- Taking an open and transparent approach – both in exercising eSafety's powers, and in terms of the information obtained through notices. eSafety will seek to make information obtained

through use of reporting notices and determinations publicly available where appropriate. eSafety recognises that the disclosure of confidential commercial information in respect of a business may have a substantial adverse effect on the interests of that business. eSafety will consider claims that certain information provided in response to a notice are commercial-in-confidence.

- Recognising the potential for regulatory burden in requests for information by taking into consideration the information that:
  - providers already publish voluntarily
  - is provided as part of international transparency initiatives
  - is provided to eSafety under another regulatory scheme.
- Recognising that differences between providers in terms of resources, technical architecture and user base, means that one size does not fit all.
- Taking a consultative approach, seeking input and feedback from providers as well as from civil society organisations, academics and other experts to ensure implementation meets standards of good regulatory practice.
- Providing additional guidance on the reasonable steps that could be taken to comply with the Expectations where needed.
- Ensuring eSafety systems securely store information, including that which is commercial-in-confidence or may contain personal information.

Implementing the Expectations

eSafety has a range of powers to seek information from service providers about their compliance with the Expectations, backed by civil penalties. eSafety is also empowered to prepare statements of compliance and non-compliance with the Expectations and publish such statements.

While the Expectations are not enforceable, it may be the case that a relevant Industry Code registered under the Act or a relevant Industry Standard, determined under the Act, may require commitments or obligations to implement the Expectations. Where this is the case, a failure to implement the Expectations may also constitute a failure to implement elements of the relevant Industry Code or Standard provided for by the Act.

There may also be circumstances where the failure to comply with an expectation under the Determination may result in other enforceable action by eSafety. For example, if a service provider has failed to comply with section 11 of the Determination to 'take reasonable steps to minimise the provision of certain material on their service', eSafety may give the provider a removal notice in relation to specific material under other parts of the Act. Failure to comply with a removal notice is a civil penalty provision and may result in a range of enforcement actions by eSafety. A demonstrated failure to comply with section 11 of the Determination is not a condition of the use of removal notices.

Additional information about eSafety's regulatory schemes and powers is available on eSafety's website.

Who do the Expectations apply to?

The Expectations apply to social media services, relevant electronic services and designated internet services accessible to Australian users. Providers should also be aware of their responsibilities under other regulatory requirements under the Act. This includes Industry Codes or Standards, which apply to a broader range of services, including app service providers, search engine service providers, internet carriage services, equipment suppliers/manufacturers and hosting providers.

Table two: The Expectations apply to three main sections within the online industry.

Section of the online industry		Scope
Social media services	Providers of social media services, so far as those services are provided to end-users in Australia.	All providers of social media services that can be accessed by end-users in Australia, including: • social networks • media sharing networks • discussion forums • consumer review networks.
Relevant electronic services	Providers of relevant electronic services, so far as those services are provided to end-users in Australia.	All providers of relevant electronic services that can be accessed by end-users in Australia, including: • email services • instant messaging services • SMS and MMS services • chat services • online games where end-users can play against each other • online dating services.
Designated internet services	Providers of designated internet services, so far as those services are provided to end-users in Australia.	All providers of designated internet services, such as websites that that can be accessed by end-users in Australia (unless a service is otherwise considered a social media service or a relevant electronic service).

What harms are covered?

The Expectations apply to all harmful content and activity covered by the Act. In addition, section 14(2) of the Determination states that providers should take responsibility for enforcing their terms of service, which may include harms that are not defined within the Act, so long as those harms are relevant to the online safety of Australians.

The Expectations specifically highlight the importance of minimising the extent to which the following content is available on a provider's service:

a. cyberbullying material targeted at an Australian child

b. adult cyber abuse material

c. a non-consensual intimate image of a person

d. class 1 material

e. material promoting, inciting, instructing in, or depicting abhorrent violent conduct.

Providers are also specifically required to take reasonable steps to prevent access by children to class 2 material.

What are the reasonable steps a provider should take?

The reasonable steps taken to comply will differ based on each expectation. The Determination does not prescribe how expectations must be met by service providers but gives examples of reasonable steps that a provider may choose to take. This provides flexibility for providers to determine appropriate means of meeting the Expectations. Providers may choose to undertake different steps but still be compliant. Providers should however be prepared to report on these steps, why they are reasonable in light of the objectives of the Determination, and how these steps meet the relevant expectation(s) and keep Australians safe.

Providers are also expected to comply with any other relevant legal obligations when implementing the Expectations, such as the Privacy Act 1988.

Further detail on the reasonable steps is included in the Explanatory Statement to the Determination. As well as these steps, implementing the applicable Industry Code, if registered, or the applicable Industry Standard, is likely to support relevant providers meeting expectations for class 1 and 2 content.

eSafety's Safety by Design principles, assessment tools and guidance materials have also been made available to enable service providers to audit and improve their current safety practices. Use of the Safety by Design assessment tools will continue to be anonymous, and eSafety will receive no information on providers' responses for the purposes of understanding compliance with the Expectations, or compliance with other regulatory schemes.

eSafety will work with relevant parts of industry and other stakeholders to develop a more detailed guide to the content of the Expectations and the reasonable steps providers may take to implement them. This further guidance will be used to support the Commissioner's judgements regarding statements of compliance and non-compliance in the future.

Consulting with eSafety on reasonable steps

Section 7 of the Determination outlines expectations in relation to consultation with eSafety.

Section 7(1) requires providers to consult with eSafety in determining what are reasonable steps for the purposes of section 6(1), which is the core expectation that end-users are able to use the service in a safe manner. As noted in the Explanatory Statement to the Determination, section 7(1) is intended to:

> **have the effect of establishing a dialogue between the Commissioner and service providers, and offers service providers the opportunity to outline the limitations to actions they can undertake to ensure safe use. For example, when reasonable steps outlined in subsection 6(3) are not appropriate for a service, that service provider may consult the Commissioner about alternative steps that could be taken to ensure safe use. It also establishes a means for information sharing so that the Commissioner and industry can share industry and social developments to improve online safety outcomes.**

Providers are expected to engage with eSafety during the drafting of further guidance on reasonable steps. In addition, where providers have specific questions regarding reasonable steps and their ability to comply, they can contact eSafety at industrybose@esafety.gov.au, although eSafety cannot provide legal advice. Providers are also expected to engage with eSafety if specific issues are identified, and a provider's willingness to engage and implement or consider eSafety's recommendations may be reflected upon when deciding whether a provider is complying with the Expectations.

Section 7(2) requires that in determining what are reasonable steps for the purposes of complying with section 6(1), a provider will have regard to any relevant guidance material made available by the Commissioner. Providers are encouraged to review this guidance, the further guidance planned on reasonable steps when published, alongside the Safety by Design tools on the eSafety website, and other materials published by eSafety.

Providing basic information, including designated contact points, to eSafety

Section 21 of the Determination requires providers to notify eSafety of a designated contact point. Any changes must be notified to eSafety in writing within 14 days after the change. Contact details may be used for engagement on implementation of the Expectations, other online safety issues, as well as a point of contact for eSafety for communications related to the enforcement of the Act. Where eSafety has existing contacts, particularly those used for content removal notices and other engagement under the Act, these are likely to continue to be used. Providers may want to nominate these existing contacts for the purposes of section 21 to ensure consistency or may choose alternative points.

In order to facilitate the sharing of contact details, and also to enable the sharing of other straightforward information, eSafety has established a webform for relevant providers. By completing and maintaining your information via this form, eSafety will regard a provider as having fulfilled the expectation under section 21.

Provision of contact information through the form is encouraged. In the future, eSafety may consider requiring companies to provide the relevant information via the webform, or another online tool.

Contact details will not be made public without the consent of providers. eSafety may request that providers share other information through the webform on a voluntary basis (for example, details of terms of use and reporting processes). Where appropriate, this information may be published in the interests of transparency.

For providers looking to obtain a webform link and share the relevant information, please contact industrybose@esafety.gov.au.

Use of industry reporting powers

Reporting and information gathering powers

A core element of the Expectations is the ability of eSafety to seek information from providers on their implementation. This information is essential in improving transparency and accountability, and also informing eSafety's decisions regarding issuing statements of compliance or non-compliance.

There are three different ways eSafety will be able to seek information from providers regarding compliance with the expectations.

1. **Requests for information**
   As part of the Expectations (section 20 of the Determination), eSafety may request information about:
   - the number of complaints about breaches of a provider's terms of use
   - the time frame for responding to removal notices
   - measures taken to make sure people can use the service in a safe manner
   - the performance of online safety measures that providers have announced publicly or reported to the Commissioner.

   While failure to comply is not enforceable, a failure to respond within 30 days would give the Commissioner discretion to prepare a statement that the service provider is not complying with the Expectations. Providers should consider whether they have processes in place to respond to these requests.

2. **Reporting notices**
   eSafety may give a reporting notice to a service provider requiring them to produce a report on their implementation in relation to any part, or the entirety of the Expectations. These notices are enforceable, backed by civil penalties and other enforcement mechanisms. Reporting notices are specific to the provider, although multiple notices can be issued. Notices can be for:
   - non-periodic reporting
   - periodic reporting over a specified time frame of between six to 24 months.

3. Reporting determinations

eSafety can make reporting determinations – a legislative instrument – requiring periodic or non-periodic reporting for a specified class of services. Like the reporting notices, these are enforceable and backed by civil penalties for failure to report.

Type of Information Gathering	Can require reporting on	Periodic or non-periodic	Reporting period	Time to respond	Enforceable
Requests for information under section 20 of the Expectations.	**1.** Terms of service complaints. **2.** The time frame for responding to removal notices. **3.** Measures taken to make sure people can use the service in a safe manner. **4.** The performance of online safety measures that providers have announced publicly or reported to the the Commissioner.	Non-periodic.	Not shorter than six months for reporting categories 1 and 2. N/A for reporting categories 3 and 4.	Within 30 days.	X
Reporting notices to **individual providers**.	Implementation of any part or the entirety of the Expectations.	Either periodic or Non-periodic.	6 to 24 months.	28 days or longer as specified.	✓
Reporting determinations to a **specified class of providers**.	Implementation of any part or the entirety of the Expectations.	Either periodic or Non-periodic.	6 to 24 months.	28 days or longer as specified.	✓

eSafety can require reporting from 24 July 2022 - six months after the Determination was registered.

In the first instance, eSafety intends to use its reporting notice powers, both non-periodic and periodic, rather than a reporting determination. eSafety is intending to expand the use of reporting powers gradually, with indicative timelines below:

- **Phase 1:** Non-periodic notices focussed on compliance with one or more specific expectations (August 2022).
- **Phase 2:** First periodic notices to begin tracking compliance with one or more expectations over time (early 2023).
- **Phase 3:** Expansion of regular reporting, any additional guidance necessary, and beginning of statements of compliance/non-compliance, and potential use of reporting determinations (2023).

Complying with a notice, determination, or request for information from eSafety

A notice or request for information is likely to be sent via email in the first instance. In the future, the ability to send and respond to notices may be integrated into an online portal.

Providers are required to answer reporting notices in the manner and form specified. A response template will be provided as part of the notice. eSafety may consider alternative formats to constitute non-compliance with the relevant notice, unless agreed to in consultation with eSafety. Providers are encouraged to engage eSafety if they cannot answer in the form specified.

Reporting notices may require information such as:

- **Qualitative information on safety tools, processes and policies, and why these are reasonable steps to implement the Expectations.** These may be phrased as yes/no questions, multiple choice questions or worded to seek descriptive information.
- **Quantitative information on the operation of safety tools, processes and policies.** This may consist of metrics to determine the impact of interventions or information about resources allocated.

Reporting notices will be related to the implementation of specific expectations. Responses will be used to understand the extent to which a service provider is fulfilling one or more Expectations and to build an understanding across different providers of common practices, trends and challenges. Given the breadth of some of the expectations, eSafety may ask questions targeted at assessing how the provider's compliance with a particular expectation minimises a specific type of harm. Our view is that targeted questions assist both the provider and eSafety. This approach ensures the provision of meaningful information and minimises the regulatory burden on respondents.

Providers are required to respond within the time frame specified. In line with the Act, this will be no shorter than 28 days from the giving of a notice, or from the end of the reporting period specified in the notice.

eSafety understands that not every expectation will apply equally to every service. If a provider is of the view that a particular expectation does not apply, they should be prepared to explain in response to a notice or determination why the provision does not apply. eSafety will consider accordingly.

Providers will also have the opportunity to engage with eSafety to identify whether any confidential material is likely to be included in their response, and also request additional time for compliance if necessary.

Where a service provider does not collect the requested information, they should endeavour to provide alternative relevant data. For example, where Australian data cannot be disaggregated from global data, the broader dataset may be acceptable.

eSafety will endeavour to inform a provider of the intention to issue a reporting notice, and the intended scope of the proposed notice, before it is given to them. This will offer the provider a time-limited opportunity (likely three to five working days) to identify any barriers to compliance within the proposed time frame of the notice. However, this may not be possible in every circumstance. For example, this might not be possible in a crisis scenario or appropriate where a provider has chosen previously not to engage with eSafety.

If a provider does not respond to a notice, eSafety has civil enforcement powers, and the power to prepare and publish a statement confirming that the provider is non-responsive.

In addition to the information provided in response to a notice, service providers can share additional information and context if they wish. However, in the interests of consistency, enforceability and transparency, where eSafety has decided that a notice is the appropriate mechanism, eSafety will not normally agree to withhold a formal notice in favour of the same information being provided via voluntary means.

How will eSafety decide which providers receive notices?

In the first instance, eSafety expects to give non-periodic notices focussing on specific expectations as they relate to acute harms, such as child sexual exploitation and abuse. When deciding which service provider(s) to serve a notice to, the Act requires eSafety to have regard for specified criteria. In deciding whether to give such a notice, eSafety must consider the following factors:[7]

- The number of complaints it has received under the Act in relation to the service in the previous 12 months.
- Any deficiencies in the provider's safety practices and/or terms of use.
- Any previous contraventions of civil penalty provisions relating to the expectations.
- Whether the provider has agreed to give the Secretary of the Department regular reports relating to safe use of their service.[8]
- Any other matters the Commissioner considers relevant.

Although not specified in the Act, examples of other matters that the Commissioner might consider relevant may include factors such as:

- Aggregated evidence from eSafety's other regulatory schemes, such as types of complaints,a platform's responsiveness to removal requests/notices, or other investigative insightsregarding platform safety issues.
- A platform's reach and the profile of its users, including whether the platform is used by children.
- The measures the platform currently has in place to protect users from harm.
- Evidence of systemic harm, or evidence of key safety issues, relative to the Expectations, including from victims, charities, media, academics, or other experts.
- The information already published by a provider, and any absence of information regarding a service's safety policies, processes and tools, or limited information about the impact or effectiveness of these interventions.

[7]Section 56(5) of the Act.
[8]This provision was included to ensure that eSafety takes into account other Australian Government reporting initiatives, and considers the burden on providers from any duplication.

The same requirements do not exist if eSafety makes a determination requiring reporting from a specified class of services. However, eSafety intends to take a similar approach to understanding risk and priority sectors for any determination.

eSafety will seek to reduce regulatory burden in reporting requirements where possible, including through eSafety's different regulatory schemes, such as the Industry Codes or Standards. For example, where providers already report information through Industry Codes or Standards, the same information will not normally be requested or required through Basic Online Safety Expectations, and vice versa.

Will information received via notices/determinations be published?

The Explanatory Memorandum to the Act highlights the intention to 'improve the transparency and accountability of online service providers for the safety of their users and the mitigation of online harms'. It further notes that:

> **The transparency reporting obligation within the BOSE [Basic Online Safety Expectations] proposal would create greater transparency of the online safety practices for both government and the community, and encourage uplift through imposing reputational costs for non-compliance.**

eSafety considers that these transparency and accountability objectives, and eSafety's broader statutory functions, will be met most effectively by making information received from industry public in response to a reporting notice, where appropriate. Service providers will be asked to:

- clearly identify in their response if any information is commercial-in-confidence or should otherwise not be published
- provide clear reasons in support of any claim that certain information is commercial-in-confidence.

eSafety will consider these claims carefully. eSafety will also consider whether there are steps than can be taken to protect such information while ensuring the transparency and accountability objectives of the Act are still met.

Information provided in response to a reporting notice may also be used by eSafety to inform other regulatory schemes, including to determine compliance with Industry Codes or Standards.

In line with the transparency objectives of the Act, eSafety also intends to publish the reporting notices, or a summary of items sought in the notices, on the eSafety website at an appropriate time. The number and type of notices, and outcomes (such as, whether it was complied with and whether any enforcement action was taken), will also be published in eSafety's annual report.

Statements of compliance/non-compliance

If eSafety decides that a service provider is not complying with one or more of the expectations, the Act empowers eSafety to prepare a statement to that effect and to publish it. eSafety may also prepare and publish a statement that confirms that a provider is meeting the Expectations in order to highlight and encourage this best practice. eSafety intends to use both powers in the future.

How will eSafety decide whether to issue a statement of non-compliance?

eSafety will take a risk-based approach when assessing whether service providers are taking reasonable steps to implement the Expectations, taking into account the level of harm and extent of the safety issues relating to a service. eSafety will also consider other factors, such as:

- Whether a provider demonstrates an effort and commitment to improving online safety for its users.
- Any particular technical or practical limits which might prevent a provider from meeting different expectations.
- Whether the provider has engaged constructively with eSafety and responded to requests for information.
- How information provided compares with evidence from other sources, such as investigative insights, as well as academic, civil society, or other expert evidence.

If a statement is prepared, eSafety will share this statement with the provider first. The provider will be given the opportunity to make further submissions, to submit additional evidence to demonstrate that it is compliant with the relevant expectation, and to comment on the statement.

eSafety intends to make statements of non-compliance public, where appropriate, in the interests of transparency and accountability.

eSafety does not intend to issue statements of non-compliance in Phase One (as detailed above) until further guidance on reasonable steps is published, other than in exceptional cases. eSafety will use the information gathered from notices to build an understanding of industry practices, relative to other sources of evidence and insight.

How will eSafety decide whether to issue a statement of compliance?

The Act requires that eSafety only issues a statement of compliance in circumstances where a service provider has met the relevant expectations at all times during a specified period. Similar to a statement of non-compliance, eSafety will take into account a number of factors when deciding whether a provider is complying with the Expectations, including:

- Evidence that a provider has implemented reasonable steps across all the relevant expectations, with evidence that these are operating effectively and consistently.
- Evidence that the reasonable steps have been taken and implemented for a reasonable time in order to evaluate their effectiveness.

- Whether the provider has engaged constructively with eSafety and responded positively to requests for information.
- How information provided by the service compares with evidence from other sources, such as investigative insights, academic, civil society or other expert evidence.

eSafety intends to publish statements of compliance on the website.

eSafety does not intend to issue statements of compliance in Phase One (as detailed above).

Review rights

Certain actions taken by eSafety relating to the Expectations can be reviewed internally by eSafety and independently by the Administrative Appeals 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.

Action which can be reviewed	Who can seek review
The issue of a non-periodic notice (Section 49 of the Act)	The provider named in the non-periodic notice
The issue of a periodic notice (Section 56 of the Act)	The provider named in the periodic notice

Additional information about seeking a review can be found on eSafety's website.

esafety.gov.au