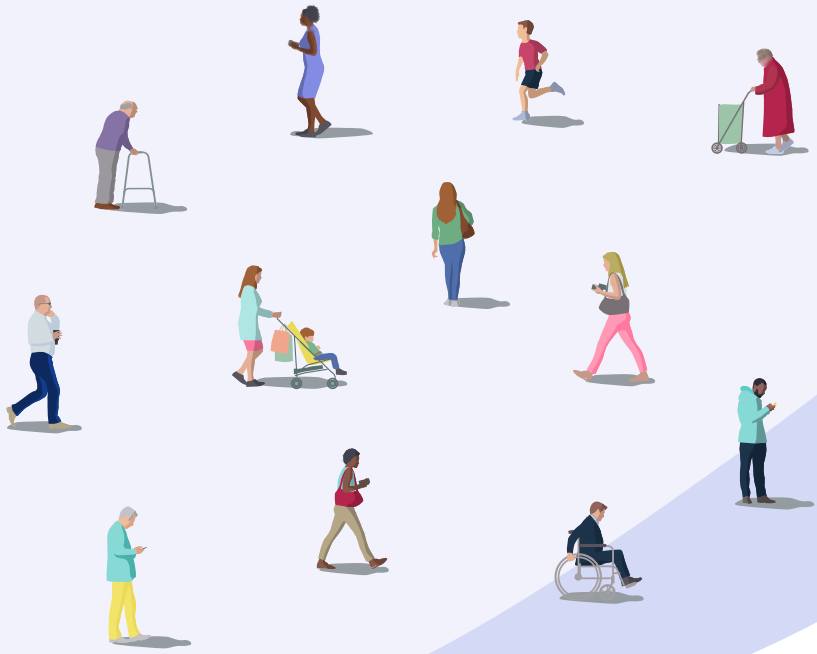
Online Safety Act 2021

Online Content Scheme

Regulatory Guidance

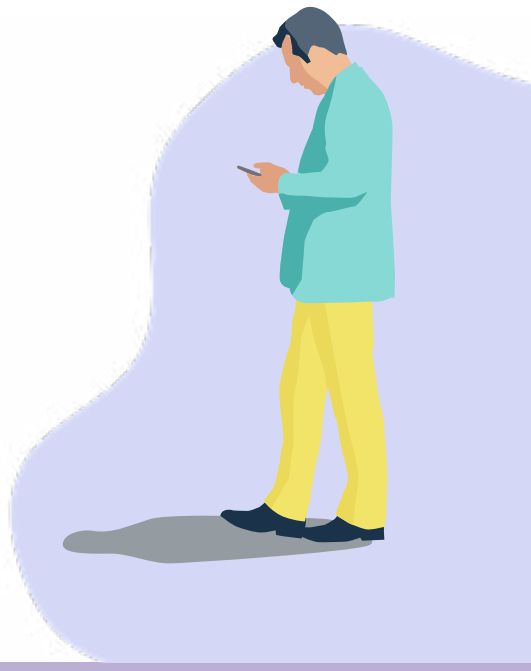
eSC RG 4

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.

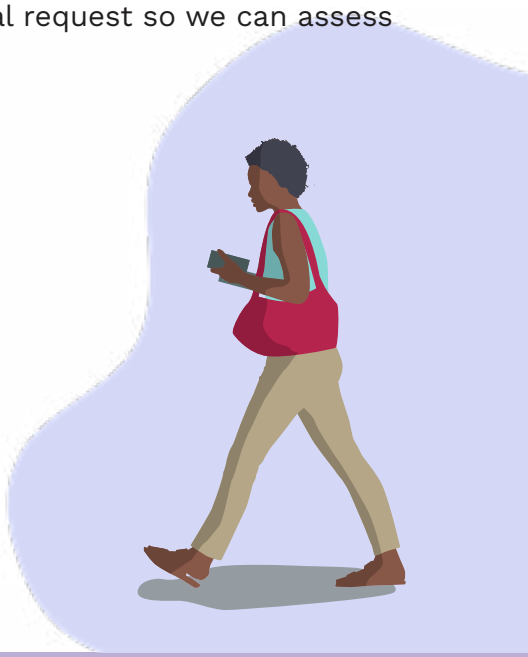
Reporting to INHOPE is enabled by a memorandum of understanding with the Australian Centre to Counter Child Exploitation. Under the memorandum of understanding, eSafety notifies INHOPE in relation to child sexual exploitation material in a member country, rather than giving a formal notice or referring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

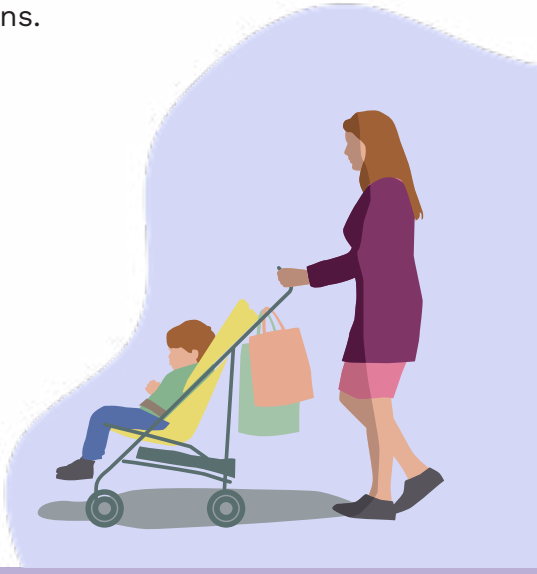
The Act does not impose any time limits within which an app removal notice must be given.

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.

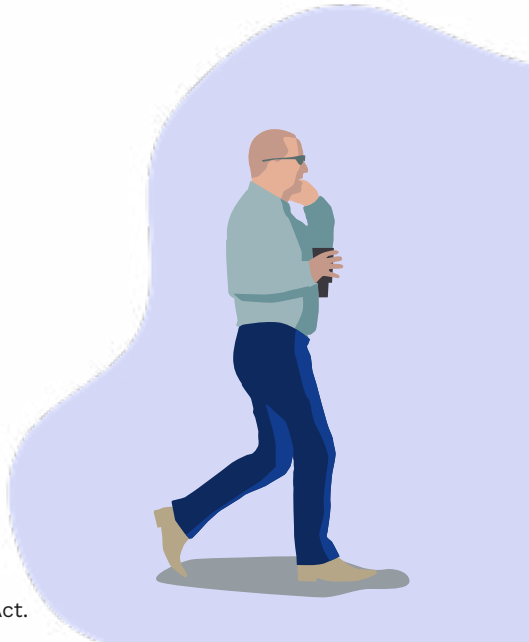
Orders to cease a service

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)