Online Safety Act 2021

Compliance and Enforcement Policy

eSC CEP

October 2024

Australian Government | eSafetyCommissioner

Contents

About this policy

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

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

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

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

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

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

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

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

Strategic context

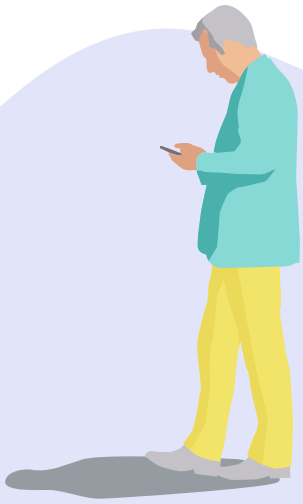
The statutory functions set out under section 27 of the Online Safety Act determine the key focus and activities of eSafety. The **eSafety Strategy 2022-2025** outlines how we will prioritise those activities to help Australians of all ages enjoy safer and more positive experiences online through until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

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

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

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

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



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

Outline of eSafety's compliance and enforcement powers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Compliance activities

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

Informal requests

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

These are examples:

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

Voluntary tools under the Act

The Act also includes some mechanisms that are not enforceable.

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

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

Civil penalty provisions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Service provider notifications: the Expectations

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

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

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

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

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

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

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

Referral of matter to law enforcement

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

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

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

General investigative powers

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

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

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

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

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

Penalties for failure to comply with the requirements of Part 13

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

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

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

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

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

Part 14 – Investigative powers

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

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

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

Penalties for failure to comply with the requirements of Part 14

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

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

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

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

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

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

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

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

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

Review rights

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

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

Enforcement action

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

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

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

Formal warnings

What is a formal warning?

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

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

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

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

When can a formal warning be given?

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

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

Will a formal warning be published?

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

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

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

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

Enforceable undertakings

What is an enforceable undertaking?

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

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

When can an undertaking be accepted?

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

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

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

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

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

What are the consequences of an enforceable undertaking?

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

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

Can an enforceable undertaking be varied or cancelled?

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

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

Injuctions

What is an injunction?

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

An injunction granted by the Court may:

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

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

When can eSafety apply for an injunction?

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

What are the consequences of an injunction?

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

Can an injunction be discharged or varied?

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

Infringement notices

What is an infringement notice?

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

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

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

Who can give an infringement notice?

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

When can an infringement notice be given?

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

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

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

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

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

Amount payable under an infringement notice

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

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

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

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

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

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

What are the consequences of an infringement notice?

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

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

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

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

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

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

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

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

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

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

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

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

Civil penalty orders

What is a civil penalty order?

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

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

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

When can eSafety apply for a civil penalty order?

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

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

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

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

What are the consequences of a civil penalty order?

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

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

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

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

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

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

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

Can a civil penalty order be appealed?

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

Federal Court orders

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

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

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

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

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

Attachment A: Enforcement options available to eSafety under the Act

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

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

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