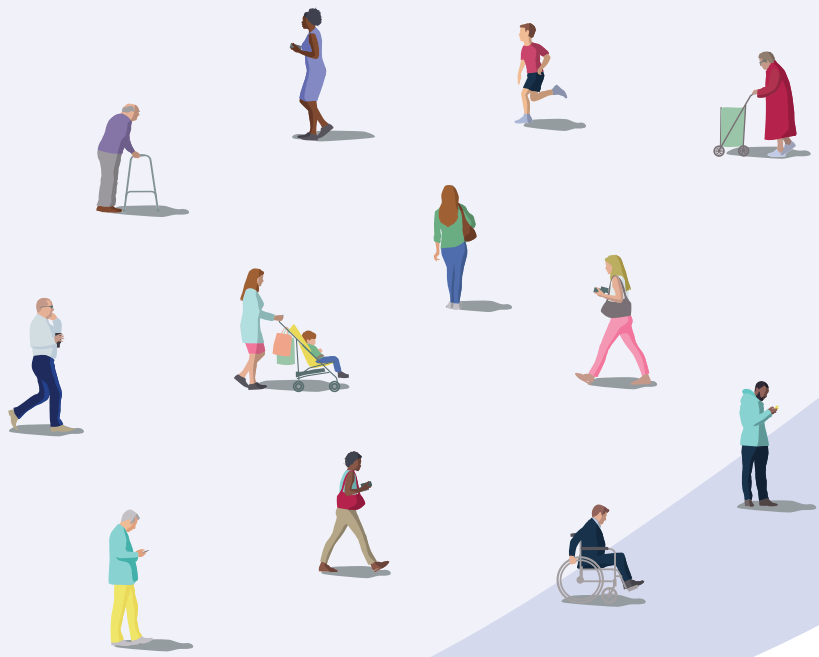
Online Safety Act 2021

Compliance and Enforcement Policy

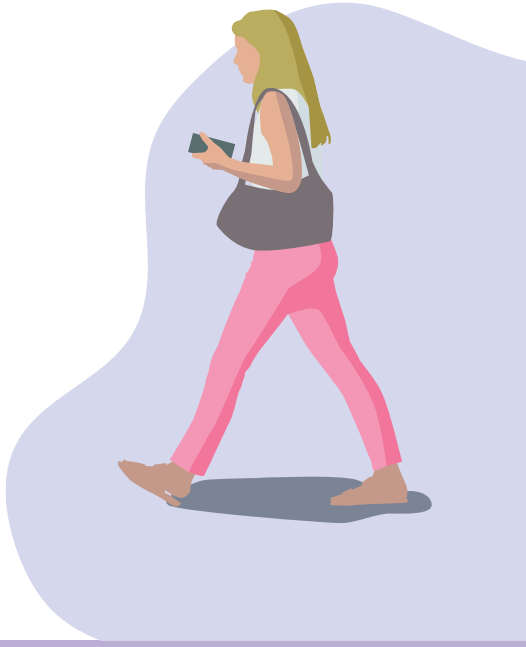
eSC CEP

December 2021



Australian Government | eSafetyCommissioner

Contents



Overview

The eSafety Commissioner (eSafety) was established as an independent statutory officeholder in 2015. In June 2021, the Australian Government enacted new legislation, the Online Safety Act 2021 (Cth) (the Act), the objects of which are to improve and promote online safety for Australians. The Act gives eSafety improved powers to help protect all Australians from the most serious forms of online harm. The Act takes effect on 23 January 2022.

This Compliance and Enforcement Policy (Policy) explains the powers available to eSafety to encourage and enforce compliance with the Act. These powers come from both the Act and the Regulatory Powers (Standard Provisions) Act 2014 (Cth) (Regulatory Powers Act).

This Policy also sets out factors that eSafety may take into account prior to using any of our powers under the Act.

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

Outline of eSafety's compliance and enforcement powers

This Policy summarises the compliance powers available to eSafety across the Cyberbullying, Image-Based Abuse, Adult Cyber Abuse and Online Content Schemes set out in Parts 5-7 and Part 9 of the Act (together, the Schemes). **Table 1** sets out an overview of each of the four Schemes and provides links to Scheme specific regulatory guidance.

The compliance actions available to eSafety across the four Schemes include:

1. **informally approaching online service providers and users of those online services (end-users)**
2. **issuing a Service Provider Notification**
3. **issuing a Removal Notice.**

In addition, other compliance actions are available to eSafety which are addressed in more detail in separate Scheme specific regulatory guidance documents.

This Policy also deals with circumstances where a provision of the Act has been breached and enforcement action is required. There are a number of options available to eSafety.[1] They include:

1. **issuing a formal warning**
2. **issuing an infringement notice**
3. **accepting an enforceable undertaking**
4. **seeking a court-ordered injunction**
5. **seeking court-ordered civil penalties.**

Each of these compliance and enforcement actions are described in more detail in this Policy.

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

In addition to the four Schemes, Part 4 of the Act articulates the Basic Online Safety Expectations, Part 8 of the Act sets out eSafety's powers to combat material which depicts abhorrent violent conduct and Part 9 contains provisions dealing with industry codes, standards and service provider determinations. These parts of the Act will be addressed in their own regulatory guidance documents and are summarised as follows:

- The Basic Online Safety Expectations encourage the prevention of online harms by online service providers by setting out the Australian government's expectations for online safety and enabling the Minister to, by legislative instrument, specify particular expectations for social media services, relevant electronic services and designated internet services.[2] The Act also empowers eSafety to require an online service provider to report on their compliance with the Basic Online Safety Expectations.[3]
- Part 8 of the Act is intended to protect the Australian community by preventing the viral online distribution of terrorist material and extreme violent material. eSafety may request or require an internet service provider to block access to material that promotes, incites, instructs or depicts abhorrent violent conduct.
- In addition to a complaint and removal scheme for illegal and restricted online content (referred to in the Act as class 1 and class 2 material), Part 9 of the Act provides a framework for guiding the creation of industry codes by bodies and associations that represent sections of the online industry. It also empowers eSafety to make industry standards if appropriate codes are not registered and to make service provider determinations that regulate certain online service providers if required. The rules set out in a determination are known as 'service provider rules'. Industry codes, standards and service provider rules are are enforceable in the following ways:
  - Members of the public can make complaints to eSafety if an industry code or standard has been breached. A breach of a direction to comply with an industry code or breach of a standard is a civil penalty provision
  - Members of the public can make complaints to eSafety if a service provider rule has been breached. A breach of a service provider rule is also a civil penalty provision.
  - eSafety is empowered to give directions aimed at ensuring an online service provider does not or will not breach a service provider rule. Failure to comply with such a direction is also a civil penalty provision.

Table 1: eSafety Complaint and Removal Schemes

Part 5 - Cyberbullying Scheme	**Part 6** - Image-Based Abuse Scheme	**Part 7** - Adult Cyber Abuse Scheme	**Part 9** - Online Content Scheme
What is it?			
This Scheme focuses on cyberbullying of Australian children across the range of online services where under 18s are spending time.	This Scheme aims to help rapidly remove intimate images that are shared without the consent of the person shown.	This Scheme aims to address material targeted at Australian adults which is both intended to cause serious harm and is menacing, harassing or offensive.	This Scheme aims to address the posting of illegal and restricted online content (referred to in the Act as class 1 and class 2 material), such as child abuse material or pro-terror content, as well as minimising children's exposure to age-inappropriate content.

[2]Online Safety Act 2021 (Cth), Part 4. [3]Online Safety Act 2021 (Cth), ss 49, 52, 56, 59.

Part 5 - Cyberbullying Scheme	**Part 6** - Image-Based Abuse Scheme	**Part 7** - Adult Cyber Abuse Scheme	**Part 9** - Online Content Scheme
Who can make a compaint?			
An Australian child who has reason to believe they were or are the target of cyberbullying material (s 30(1) of the Act). Or a responsible person who has reason to believe that cyberbullying material was or is targeted at an Australian child and they are the child's parent or guardian or authorised by the child to make the complaint (s 30(2) of the Act). Or an Australian adult 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) (s 30(3) of the Act).	A person[4] depicted in an intimate image who has reason to believe s 75 of the Act[5] has been contravened (s 32(1)-(2) of the Act). Or a person authorised on behalf of the person shown in the intimate image. This includes parents or guardians of children who have not reached 16 years and parents or guardians of a person who is incapable of managing their own affairs (s 32(3)-(5) of the Act).	An Australian adult who has reason to believe that they were or are the target of adult cyber abuse material (s 36(1) of the Act). Or a responsible person who has reason to believe that adult cyber abuse material was or is targeted at an Australian adult and has been authorised to make the complaint on behalf of the adult (s 36(2) of the Act).	A person who has reason to believe that Australians can access class 1 and certain class 2 material through an online service provider[6] (s 38(1) of the Act). Or a person who has reason to believe that Australians can access certain class 2[7] material through an online service provider and that access is not subject to a restricted access system (s 38(2) of the Act).
Complaints process			
Complaints can be made in relation to cyberbullying. If the complainant wants eSafety to give a removal notice, the complaint must be accompanied by evidence that shows the complainant has complained to the relevant online service provider already. eSafety cannot issue a removal notice until at least 48 hours have passed since this complaint (ss 30(4), 65 and 66 of the Act).	Complaints can be made about non-consensual posting (or threats of posting) of intimate images (s 32 of the Act). Objection notices can be given for intimate images including where the images were initially posted with consent (s 33 of the Act).	Complaints can be made in relation to adult cyber abuse material. If the complainant wants eSafety to give a removal notice, the complaint must be accompanied by evidence that shows the complainant has already complained to the online service provider. eSafety cannot issue a removal notice until at least 48 hours have passed since this complaint (ss 36(3), 88, 89 and 90 of the Act).	Complaints can be made in relation to class 1 and class 2 material (s 38 of the Act). eSafety can conduct, on our own initiative or in response to a complaint under s 38, investigations it considers desirable (s 42 of the Act).

[4]Either the person depicted or the person who is posting or threatening to post the intimate image must be ordinarily resident in Australia. [5]Section 75 of the Act prohibits posting or threatening to post an intimate image without the consent of the person shown in the images. [6]Class 1 material is defined in s 106 of the Act and class 2 material is defined in s 107 of the Act. [7]Material that is or would likely be classified as R18+ or Category 1 restricted.

Part 5 - Cyberbullying Scheme	**Part 6** - Image-Based Abuse Scheme	**Part 7** - Adult Cyber Abuse Scheme	**Part 9** - Online Content Scheme
Compliance options available			
• Service provider notifications (s 73 of the Act) • Removal notices (ss 65 and 66 of the Act) • End-user notices (s 70 of the Act)	• Service provider notifications (s 85 of the Act) • Removal notices (ss 77-79 of the Act) • Remedial directions (s 83 of the Act)	• Service provider notifications (s 93 of the Act) • Removal notices (ss 88-90 of the Act)	• Service provider notifications (ss 113A, 118A, 123A of the Act) • Removal notices (ss 109, 110, 114, 115, of the Act) • Remedial notices (ss 119-120 of the Act) • Link deletion notices (s 124 of the Act) • App removal notices (s 128 of the Act)
Enforcement options			
See **Attachment A**			
Scheme-specific regulatory guidance			
Cyberbullying Scheme Regulatory Guidance	Image-Based Abuse Scheme Regulatory Guidance	Adult Cyber Abuse Scheme Regulatory Guidance	Online Content Scheme Regulatory Guidance

Considerations eSafety takes into account when determining compliance or enforcement action

eSafety takes a graduated approach, where appropriate, to compliance and enforcement that strives to balance the protection of Australians with ensuring no undue burden is imposed on online service providers and individuals. eSafety's starting point when determining what initial action to take is that informal or less intrusive action is preferred, if appropriate in the circumstances and likely to achieve the desired regulatory result. The types of decisions that eSafety makes in exercising our compliance and enforcement functions include:

- whether it is appropriate or desirable to exercise our discretion to take no action
- whether to commence an investigation
- whether compliance or enforcement action is appropriate in the circumstances
- what is the most effective way to facilitate the removal of harmful material

- whether to direct regulatory action towards an individual responsible for harmful material or conduct
- what, if any, investigative and/or information gathering powers should be used and how
- whether extending the time for compliance with a notice, direction or similar action under the Act (for example the 24 hour period to comply with a removal notice) is appropriate.

The action eSafety takes will always depend on the facts and the circumstances of each case. Relevant factors that might be considered include:

- the best interests and preferences of the person targeted by harmful material or conduct, including any safety concerns and any potential risks to the person targeted
- the nature, context and content of the relevant material and the severity of its impact and harm
- the need to alleviate harm as quickly as possible, including the risk of potential harm or further harm from allowing the post to remain online (for example, a post doxing a person and including an allegation of criminality potentially creates a more imminent and serious risk of harm to that person than a post that only alleges criminality but contains no personal information)
- the number of posts and the extent of distribution of any material
- the supporting evidence available or able to be obtained
- the circumstances of the person targeted by the material, including age and any indicators of vulnerability
- the extent to which any informal avenues may be available or suitable to address the situation, and whether such approaches have been successful in similar circumstances
- the educative or deterrent effect of taking certain action
- whether the identity and contact details of relevant entities or persons required to take the action are known or can be established
- the likelihood that action will result in compliance
- whether the intended subject of the regulatory action has been the subject of prior compliance or enforcement action, and the outcome of that action
- whether the conduct is the subject of a police investigation or other process and, if so, any effect that the proposed action may have on this investigation or process
- any potential risk of undermining public confidence in eSafety to perform the required functions under the Act
- the extent to which any conduct represents a broader systemic issue
- the burden on the person who will be the subject of regulatory action
- the public interest (including any educational merit) in the material remaining available
- the extent to which the material is or should be protected by s 233 of the Act[8] or under the concept of free speech generally
- any other factors that eSafety considers to be of relevance.

[8]Section 233 of the Act provides that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.

In addition, in determining whether to take compliance or enforcement action against an **end-user**, eSafety may also consider:

- whether eSafety can establish and verify the identity and contact details of the end-user
- the circumstances of the end-user, such as age, any indicators of vulnerability and level of support required to respond to compliance or enforcement action
- if the end-user is a child, the desire for compliance or enforcement action against that child to be the least severe option that is available and appropriate in the circumstances
- the relationship between the end-user and the person targeted by the material, and any safety concerns or other issues or risks that might arise if action is taken against the end-user
- whether the posting of the material was part of a broader course of conduct on the part of the end-user
- whether the conduct was deliberate, reckless or inadvertent
- whether the end-user has taken any action in an attempt to mitigate or address the detriment to the person targeted by the material
- whether the matter can be resolved more quickly or easily by taking action through an online service provider
- any other factors that eSafety considers to be of relevance.

In addition, in determining whether to take compliance or enforcement action against the **online service provider**, eSafety may also consider:

- whether eSafety is able to establish and verify the identity and contact details of the online service provider required to take the action
- the methods of contact that are available to eSafety, and the suitability of those methods for the proposed action
- whether the online service provider was aware of the material
- whether there is other material available on the service which breaches the Act
- the size, maturity and capability of the online service provider
- whether the service or online service provider solicits such material or otherwise promotes it
- whether the service or online service provider obtains financial or other benefits as a result of such material
- the responsiveness and level of cooperation of the online service provider in relation to any prior compliance or enforcement action
- any other factors that eSafety considers to be of relevance.

Compliance options

Informal approaches

eSafety will consider taking informal compliance action where appropriate.

While the Schemes give eSafety powers to seek the removal of material using formal notices, we will usually seek to approach the relevant online service provider or end-users informally in the first instance. This generally results in faster removal of material, compared to formal methods. In turn, this can provide a better outcome for our complainants.

However, eSafety will not hesitate to use our formal powers when we consider it appropriate.

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

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

Removal notices

What is a removal notice?

A removal notice is a written notice requiring the removal of specified material.

A removal notice may be issued to an individual end-user[9] (except in the Online Content Scheme[10] and the Cyberbullying Scheme[11]) or to the provider of a social media service, relevant electronic service, designated internet service or hosting service provider (in all of the Schemes).[12]

Generally, a removal notice requires the recipient to take all reasonable steps to remove material[13] notified by eSafety. A failure to do so is a breach of a civil penalty provision.[14]

[9]Online Safety Act 2021 (Cth), ss 70, 78 and 89. [10]Under the Online Content Scheme, unique notices can also be issued to the provider of an internet search engine service (Online Safety Act 2021 (Cth), ss 128-131) or app distribution service (Online Safety Act 2021 (Cth), ss 124-127) in certain circumstances. [11]The Cyberbullying Scheme contains a unique end-user notice which can require a recipient to take action over and above removal, s 70 Online Safety Act 2021 (Cth). [12]Online Safety Act 2021 (Cth), ss 65, 66, 77, 79, 88, 90, 109, 110, 114, 115. [13]Except for s 65 of the Act, under which a removal notice includes an absolute requirement to remove of the material (rather than a requirement to take reasonable steps to do so). [14]Online Safety Act 2021 (Cth), ss 67, 80, 91, 111, 116.

When can a removal notice be issued?

Under the Act, eSafety may issue a removal notice in any of the following circumstances:

- **Cyberbullying Scheme:** for the removal of cyberbullying material targeting an Australian child, where a valid complaint has been made to eSafety.
- **Image-Based Abuse Scheme**: for the removal of an intimate image shared without the consent of the person shown where:
  - a valid complaint has been made to eSafety, or
  - a valid objection notice has been given to eSafety.
- **Adult Cyber Abuse Scheme**: for the removal of adult cyber abuse material targeting an Australian adult, where a valid complaint has been made to eSafety.
- **Online Content Scheme**: for the removal of illegal or restricted online content,[15] where a valid complaint has been made to eSafety or eSafety has commenced an investigation on our own motion.

A removal notice must identify the relevant material in a way that is sufficient to enable the online service provider or end-user to comply with the notice. This may include eSafety providing URLs, screen shots or time stamps.

In all cases, the recipient of the removal notice must endeavour to remove the material within 24 hours after the notice is given.[16]

eSafety has the discretion to consider an extension of the 24-hour removal period. The Act does not provide any limits on what eSafety may consider when providing an extension, although eSafety will be guided by the factors set out at **Page 6**.

The Act does not set a time limit within which eSafety must issue a removal notice.

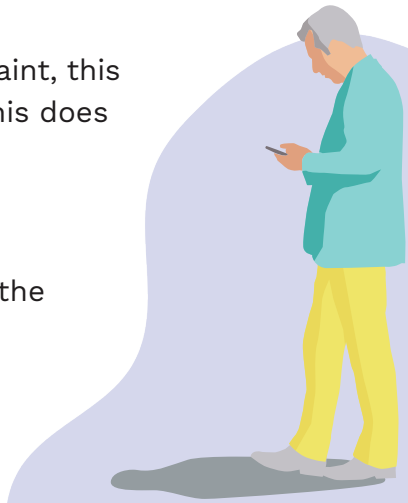
Review rights

eSafety's decision to issue a removal notice is subject to internal review by eSafety and external Administrative Appeal Tribunal (AAT) merits review.[17]

If eSafety refuses to issue a removal notice following a valid complaint, this decision is also subject to internal review and AAT merits review (this does not apply in relation to the Online Content Scheme).[18]

What are the consequences of a removal notice?

A recipient must comply with a removal notice to the extent that the person is capable of doing so.[19]



[15]Material which is classified or likely to be classified X18+ or Category 2 restricted. [16]See e.g. Online Safety Act 2021 (Cth), s 65(1)(g)(i). [17]Online Safety Act 2021 (Cth), ss 220, 220A. [18]Online Safety Act 2021 (Cth), ss 220, 220A. [19]See Online Safety Act 2021 (Cth), ss 67, 80, 91, 111, 116.

Where a person fails to comply with a removal notice, eSafety may:

- issue a formal warning
- issue an infringement notice
- accept and enforce undertakings to ensure compliance with a removal notice
- seek a court-ordered injunction
- seek a court-ordered civil penalty order.

Scheme-specific information

For more information about how removal notices are used in the context of each Scheme, please see the following regulatory guidance:

- **Cyberbullying Scheme Regulatory Guidance**
- **Image-Based Abuse Scheme Guidance**
- **Adult Cyber Abuse Scheme Guidance**
- **Online Content Scheme Guidance**

Service provider notifications

What is a service provider notification?

A service provider notification is a statement prepared by eSafety which is given to the provider of an online service and in some circumstances may be published on eSafety's website. 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.

These notifications can be used in the following circumstances:

1. If eSafety is satisfied that certain material in relation to which a complaint has been made (or an objection notice has been given) to eSafety is available on a service, eSafety may (with the consent of the complainant) alert the service by written notice.[20] This option is available for material falling within the Cyberbullying, Image-Based Abuse and Adult Cyber Abuse Schemes.

2. If eSafety is satisfied that there were two or more occasions during the previous 12 months on which certain material (the subject of the four Schemes) is, or was, available on a provider's service in breach of the service's terms of use, eSafety may provide a statement to this effect to the online service provider. eSafety is also empowered to publish the statement on our website.[21] This option is available under all four Schemes. eSafety will generally look to give an online service provider a chance to comment (and take action) before the need to publish these statements arises.

The second type of service provider notifications will be used to encourage online service providers to comply with the Act in order to avoid negative publicity (sometimes referred to as 'name and shame' powers).

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

[20]Online Safety Act 2021 (Cth), ss 73(1), 85(1), 93(1). [21]Online Safety Act 2021 (Cth), ss 73(2), 85(2), 93(2), 113A, 118A, 123A.

What are the consequences of a service provider notification?

A failure to take action after receiving a service provider notification does not attract any penalties or give rise to other enforcement options. However, eSafety expects that an online service provider would cooperate with the notification and remove the content without the need for eSafety to resort to more formal action.

In addition, eSafety will take into account an online service provider's response to a service provider notification when considering what steps to take, both in respect of the immediate circumstances and in the future in relation to material on that service.

Enforcement powers

The following powers are available once a specific provision has been breached. See **Attachment A** for a list of all the relevant provisions under the Act and which enforcement options apply.

Formal warnings

What is a formal warning?

A formal warning is used 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.[22] In addition, formal warnings can be issued for a breach of a provision of an industry code or standard registered under the Act,[23] or where eSafety is satisfied that the provider has breached a service provider rule that applies to them.[24] A formal warning can also signal that stronger enforcement action may be taken if the breach is not rectified or there are further breaches.

Formal warnings were included in the various Schemes under the Act in order to provide eSafety with an educative mechanism for addressing non-compliance.

In line with eSafety's graduated and proportionate approach to enforcement, eSafety considers that a formal warning may be appropriate where there are no aggravating features involved in a matter. eSafety may also rely on formal warnings when dealing with breaches of the Act by minors.

Further, there may be instances where it is appropriate to issue a formal warning in matters involving more significant and serious conduct 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 issued?

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

[22]Online Safety Act 2021 (Cth), ss 51, 54, 58, 61, 68, 72, 76, 81, 84, 92, 112, 117, 122, 126, 130. [23]Online Safety Act 2021 (Cth), ss 144, 147.
[24]Online Safety Act 2021 (Cth), s 155.

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.

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

A formal warning notifies the recipient that they have breached a civil penalty provision or other provision of the Act[25] but does not compel any action from them. There are no penalties that can be imposed for inaction following the receipt of a formal warning.

Nevertheless, 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 to act, or refrain from acting, in a particular manner to ensure compliance with the Act. Once eSafety accepts an undertaking, it becomes enforceable by a court. Enforceable undertakings provide a flexible opportunity for a person involved in, or responsible for, non-compliance with the Act to be engaged in resolution of the matter.

If eSafety is able to engage with an end-user or online service provider, 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 in relation to an end-user or online service provider that has failed to comply with a civil penalty provision specified in s 164(1) of 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 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.

What does an enforceable undertaking contain?

An enforceable undertaking must be in writing and must be expressed to be an undertaking under s 114 of the Regulatory Powers Act.

[25]See **Attachment A** for list of provisions which can give rise to a formal warning.

eSafety may accept an undertaking that a person will:

- take specified action in order to comply with one of the provisions specified in s 164(1) of the Act[26]
- refrain from taking specified action in order to comply with one of the provisions specified in s 164(1) of the Act,[27] or
- take specified action directed towards ensuring that the person does not contravene one of the provisions specified in s 164(1) of the Act, or is unlikely to contravene such a provision, in the future.[28]

What are the consequences of an enforceable undertaking?

If eSafety considers that a person has breached an enforceable undertaking, eSafety may apply to a court for:[29]

- 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.

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.[30]

eSafety may, by written notice, cancel the undertaking.[31]

Injunctions

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.[32] eSafety can seek an injunction in the Federal Court of Australia or Federal Circuit Court of Australia.[33]

An injunction 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[34]

[26]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(a). [27]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(b). [28]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(c). [29]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 115. [30]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(3). [31]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(5). [32]The sections which can be subject to an injunction under the Act are set out in s 165(1) of the Act. [33]Online Safety Act 2021 (Cth), s 165(3). [34]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 121(1)(a).

- require a person who has contravened, is contravening or is proposing to contravene a relevant provision of the Act to take a specific action[35]
- 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.[36]

When can eSafety apply for an injunction?

The provisions of the Act which can be subject to an injunction are set out in s 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.[37]

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 action being taken.

If an infringement notice is paid, eSafety cannot pursue proceedings seeking a civil penalty order for that specific contravention of the Act.[38] However, such proceedings may follow if an infringement notice is not paid.

Payment of an infringement notice is not an admission of liability.[39]

Who can give an infringement notice?

An infringement officer is empowered to issue an infringement notice.[40] 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 eSafety to give an infringement notice.[41]

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 s 163(1) of the Act (see **Attachment A** for more detail).[42] eSafety considers that, generally, an infringement notice will be best suited for matters where eSafety determines that the breach of the Act is relatively minor and that a financial penalty may deter future non-compliance with the Act.

[35]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 121(1)(b). [36]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 121(2). [37]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 123. [38]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 107. [39]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 107(e). [40]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 101. [41]Online Safety Act 2021 (Cth), s 163(2). [42]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 103(1).

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.

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.[43]

What does an infringement notice need to contain?

Infringement notices are governed by the Regulatory Powers Act and are required to include (among other things):[44]

- details of the infringement officer who has issued the infringement notice
- details about the alleged contravention(s)
- a dollar amount that must to be paid in order to satisfy the notice
- the time frame in which that amount must be paid to avoid civil penalty proceedings
- a statement to the effect that payment of the amount is not an admission of liability
- the options available to a person receiving the notice, including the effects of paying the amount and the steps available to seek withdrawal of the notice.

Amount payable under the infringement notices

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

If the notice relates to one alleged contravention, the penalty amount will be:[45]

- 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.[46]

At the time of the Act's commencement (23 January 2022), one penalty unit amounts to $222.[47] This means that a recipient of an infringement notice would be required to pay:

- if the person is an individual – $2,664 for every alleged contravention
- if the person is a body corporate – $13,320 for every alleged contravention.

[43]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 103(2). [44]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104. [45]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104(2). 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 for 500 penalty units, the lesser of those two options will always be the latter option. [46]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104(3). [47]The relevant penalty unit value will be that applicable at the time of the contravention at issue.

What are the consequences of an infringement notice?

If the recipient of the infringement notice pays the specified penalty within 28 days, their liability is discharged. Court proceedings seeking a civil penalty order may not be brought in relation to the alleged contravention.[48]

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 penalty. eSafety or a delegate may, in their discretion, extend that period. More than one extension may be given.[49]

If the penalty is not paid, eSafety may commence civil penalty proceedings. The court would determine whether the alleged contravention(s) has been established and, if so, the appropriate penalty. The maximum civil penalty under the Act is 500 penalty units for an individual and 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.

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

Yes. The recipient of an infringement notice can write to eSafety or a delegate and seek to have the notice withdrawn.[50] eSafety or a delegate may also withdraw an infringement notice of their own volition.[51]

When deciding whether or not to withdraw an infringement notice eSafety or a delegate:[52]

- must take into account any written representations from the recipient seeking the withdrawal
- 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 penalty proceedings against the person in relation to the alleged contravention(s).[53]

[48]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 107(1). [49]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 105.
[50]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(1). [51]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(2).
[52]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(3). [53]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104(1)(m).

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 Commonwealth 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 where the person has caused significant harm, has engaged in multiple contraventions or other compliance and enforcement options have been ineffective. Before seeking a civil penalty order against a person eSafety may take into account the person's circumstances, including any vulnerabilities or disadvantages.

Who can apply for a civil penalty order?

eSafety is authorised to apply for a civil penalty order in the Federal Court of Australia or Federal Circuit Court of Australia.[54]

When can the Commissioner apply for a civil penalty order?

eSafety can commence court proceedings seeking a civil penalty order against a person – whether 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 civil penalties 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.[55]

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 Commonwealth such pecuniary penalty as determined to be 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.[56]

Most provisions specify a maximum penalty of 500 penalty units for individuals. 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.

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.[57]

[54]Online Safety Act 2021 (Cth), ss 162(2)-(3). [55]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 82(2). [56]Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 82(5). [57]Online Safety Act 2021 (Cth), ss 195, 205(2) and 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.

The following table shows the potential maximum penalty amounts, as at 23 January 2022, per contravention.[58]

Who?	100 penalty units (x5 for body corporate)	500 penalty units (x5 for body corporate)
Individual	$22,200	$111,000
Body corporate	$111,000	$555,000

Image-based abuse and adult cyber abuse closely align to the aggravated offence of using a carriage service to menace, harass or cause offence (involving private sexual material). This is an offence contrary to 474.17A of the Criminal Code 1995 (Cth) (Criminal Code).

In addition, in relation to any prosecution for an offence under s 474.17A of the Criminal Code, it is a special circumstance of aggravation if an individual has been subject to three or more civil penalty orders arising from:

- contraventions of the general prohibition against image-based abuse, or
- failure to comply with an adult cyber abuse removal notice.

In these circumstances the maximum penalty will be increased.

Any such criminal proceedings will be conducted by either police or the Commonwealth Director of Public Prosecutions.

Can a civil penalty order be appealed?

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

Referral of matter to law enforcement

There are a number of Commonwealth and state/territory criminal offences that may apply to online harms. Where eSafety becomes aware of material that is sufficiently serious, eSafety must refer the matter to the relevant police force.

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

Under s 90 of the Regulatory Powers Act, criminal proceedings may be commenced against a person for conduct that is the same or substantially the same as conduct in respect of which a civil penalty order has been made.

[58]The relevant penalty unit value will be that applicable at the time of the contravention at issue.

General investigative powers

eSafety has considerable discretion in how we conduct investigations. The Act provides eSafety with powers to summon a person for examination and to compel the giving of information and the production of documents.

Part 13 – Information Gathering Powers

If eSafety believes on reasonable grounds that an online service provider[59] has:

- the contact details or other information about the identity of an end-user of the service, and
- this information is relevant to the operation of the Act,

eSafety can issue a written notice requiring the provision of that information (s 194 Notice).[60]

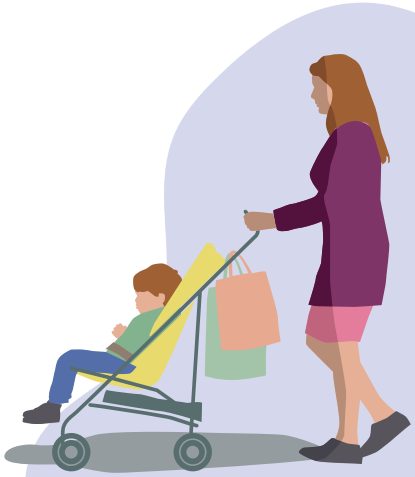
eSafety can set the time period for complying with a s 194 Notice, as well as the manner and form in which the information should be provided.[61]

Penalties for failure to comply with the requirements of Part 13

A person who does not comply with a s 194 Notice is in breach of a civil penalty provision, with an applicable civil penalty of up to 100 penalty units for an individual. The maximum penalty that can be ordered against a corporation (which can include online service providers) can be five times more than the maximum penalty ordered against individual.

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

- the significance or triviality of any refusal to comply
- the extent to which the refusal to comply has undermined eSafety's functions and powers
- 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 complainants
- any of the other relevant factors specified at **Page 6**.



[59]A provider of a social media service, a relevant electronic service or a designated internet service (s 194(1)(a) of the Online Safety Act 2021 (Cth)). [60]Online Safety Act 2021 (Cth), s 194(1).
[61]Online Safety Act 2021 (Cth), s 194(2).

Part 14 – Compulsory examination and document production powers

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

- attend before eSafety (or a delegate) to produce documents or to answer questions[62] or to provide other information[63]
- make available for inspection by eSafety (or a delegate) any documents in the possession of the person that may contain information relevant to the subject matter of an investigation[64]
- permit eSafety (or a delegate) to make copies of any such documents.[65]

These powers only apply to matters relevant to an investigation under ss 31, 34, 37 or 42 of the Act.[66] These sections relate to investigations resulting from complaints under the four Schemes in the Act, as well as eSafety's investigations (on our own motion) under the Online Content Scheme.

Procedures

A person who gives evidence or produces documents at an examination by eSafety has the same protection as a witness in a proceeding in the High Court.[67]

If a person is summoned to attend before eSafety to answer questions or make statements, eSafety can require that person to take an oath or make an affirmation that the statements the person will make will be true to the best of the person's knowledge or belief.[68]

eSafety may also require a person to answer a question that is relevant to a matter that eSafety is investigating or is planning to investigate.[69]

These examinations will occur in private, and a person who is being examined may have an adviser present.[70]

A record must be kept of any examination under this Part of the Act. The person who is under examination is entitled to a copy of the record.[71]

[62]Online Safety Act 2021 (Cth), s 199(a). [63]Online Safety Act 2021 (Cth), s 199(b) [64]Online Safety Act 2021 (Cth), s 203(a). [65]Online Safety Act 2021 (Cth), s 203(b). [66]Online Safety Act 2021 (Cth), s 198. [67]Online Safety Act 2021 (Cth), s 204. [68]Online Safety Act 2021 (Cth), ss 200(1)-(2). [69]Online Safety Act 2021 (Cth), s 200(3). [70]Online Safety Act 2021 (Cth), s 201. [71]Online Safety Act 2021 (Cth), s 202.

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:[72]

- 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, or
- refuse or fail to produce a document that the person is required to produce.

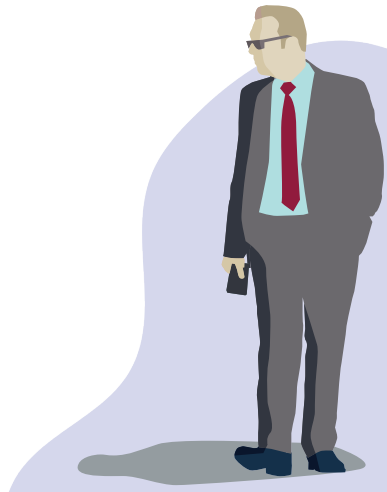
The criminal offence carries a maximum penalty of 12 months imprisonment, while the civil penalty provision carries a maximum penalty of 100 penalty units.[73]

However, it is not an offence or a breach if:[74]

- the person can show that they have a reasonable excuse for the refusal, or
- the answer to the question or the production of the document would tend to incriminate the person, or
- 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 whether, in response to a refusal to comply with the requirements of Part 14, to commence civil penalties proceedings or refer the matter to the Australian Federal Police or Commonwealth Director of Public Prosecutions, eSafety will consider, amongst other things:

- the significance or triviality of any refusal to comply
- the extent to which the refusal to comply has undermined eSafety's functions and powers
- 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 complainants
- any of the other relevant factors specified at **Page 6**.



[72]Online Safety Act 2021 (Cth), s 205. [73]Online Safety Act 2021 (Cth), ss 205(1)-(2). 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. [74]Online Safety Act 2021 (Cth), ss 205(3)-(5).

Attachment A: Compliance and Enforcement Options Available to eSafety under the Act

Section	Provision	Civil Penalty[75]	Formal warning	Infringement notices	Enforceable undertakings	Injunctions
Part 4 – Basic Online Safety Expectations						
50	Non-compliance with periodic reporting notice	500 penalty units	Section 51: For contravention of s 50	✓	✓	✓
53	Non-compliance with periodic reporting determination	500 penalty units	Section 54: For contravention of s 53	✓	✓	✓
57	Non-compliance with non-periodic reporting notice	500 penalty units	Section 58: For contravention of s 57	✓	✓	✓
60	Non-compliance with non-periodic reporting determination	500 penalty units	Section 61: For contravention of s 60	✓	✓	✓
Part 5 – Cyberbullying Scheme						
67	Non-compliance with removal notices to SMS, DIS, RES[76] and hosting service providers	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	Posting/threatening to post an intimate image	500 penalty units	Section 76: For contravention of s 75	✓	✓	✓
80	Non-compliance with removal notices SMS, DIS, RES, hosting service providers and end-users)	500 penalty units	Section 81: For contravention of s 80	✓	✓	✓
83	Non-compliance with remedial direction (person posting or threatening to post)	500 penalty units	Section 84: For contravention of s 83	✓	✓	✓
Part 7 – Adult Cyber Abuse Scheme						
91	Non-compliance with removal notices (SMS, DIS, RES, hosting service providers and end-users)	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	✗	✗	✓	✓

[75]Note that the maximum penalty ordered against a corporation (which can include online service providers) can be five times more than the maximum penalty listed here: Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 82(5). [76]SMS, DIS, RES in this table means: Social Media Service, Designated Internet Service and Relevant Electronic Service.

Section	Provision	Civil Penalty[75]	Formal warning	Infringement notices	Enforceable undertakings	Injunctions
Part 9 – Online Content Scheme						
111	Non-compliance with Class 1 removal notice (SMS, DIS, RES, hosting service providers)	500 penalty units	Section 112: For contravention of s 111	✓	✓	✓
116	Non-compliance with Class 2 removal notice (SMS, DIS, RES, hosting service providers)	500 penalty units	Section 117: For contravention of s 116	✓	✓	✓
121	Non-compliance with Class 2 remedial notice (SMS, DIS, RES, hosting service providers)	500 penalty units	Section 122: For contravention of s 121	✓	✓	✓
125	Non-compliance with link deletion notice	500 penalty units	Section 126: For contravention of s 125	✓	✓	✓
129	Non-compliance with app removal notice	500 penalty units	Section 130: For contravention of s 129	✓	✓	✓
143	Non-compliance with industry codes	500 penalty units	Section 144: For contravention of s 143	✓	✓	✓
146	Non-compliance with industry standards	500 penalty units	Section 147: For contravention of s 146	✓	✓	✓
153	Non-compliance with service provider rules	500 penalty units	Section 155	✗	✗	✗
154	Contravention of a remedial direction – breach of service provider rules	500 penalty units	✗	✗	✗	✗
Part 13 – Information-gathering powers						
195	Non-compliance with removal notices (SMS, DIS, RES, hosting service providers and end-users)	100 penalty units	✗	✗	✗	✓
Part 14 – Investigative powers						
205	Non-compliance with a blocking notice	Criminal penalty: Imprisonment for 12 months; Civil penalty: 100 penalty units	✗	✗	✗	✗

esafety.gov.au