Online Safety Act 2021

Adult Cyber Abuse Scheme

Regulatory Guidance

eSC RG 3

Updated December 2023

Australian Government | eSafetyCommissioner

Contents

Overview of this guidance

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

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

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

Overview of the Adult Cyber Abuse Scheme

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

1. **A system under which a person may make a complaint to eSafety** about adult cyber abuse material that targets an Australian who is 18 years or older. A complainant must have first reported the abuse to the relevant online service provider before eSafety can give a notice requiring removal of adult cyber abuse material.

2. **Investigative and information gathering powers** which allow eSafety to assess complaints of adult cyber abuse and decide what action we can take.

3. **Removal powers** which allow eSafety to give notices to online service providers, and to people (end-users) who have posted, shared or sent adult cyber abuse material, requiring them to remove the material. eSafety's removal powers only come into effect if a complaint has been made directly to an online service provider and they have failed to remove the material.

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

Key terms

What is 'adult cyber abuse'?

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

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

1. intended to cause serious harm, and

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

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

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

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

Who is meant by 'a particular Australian adult'?

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

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

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

[1]Section 7 of the Act.

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

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

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

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

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

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

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

What is meant by 'mere ordinary emotional reactions'?

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

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

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

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

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

What does 'menacing, harassing or offensive' mean?

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

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

Menacing or harassing

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

Offensive

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

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

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

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

[3]Section 8 of the Act.

Freedom of speech

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

The Act balances these important concepts in two main ways:

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

Material that does not meet the threshold

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

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

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

Making a complaint to eSafety

Who can complain?

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

[4]Section 233 of the Act.

Complaint made by an Australian adult

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

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

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

Complaint made on behalf of an Australian adult

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

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

Making a complaint to online service providers first

Before eSafety can give a removal notice for adult cyber abuse material, the person making the complaint must show that they have already made a complaint about the material to the relevant online service provider.[8] We will ask for this evidence through our online reporting form. eSafety cannot give a removal notice until at least 48 hours have passed since the report was made to the relevant online service provider.[9]

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

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

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

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

Investigation of adult cyber abuse material

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

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

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

Prioritising Complaints

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

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

Approaches to compliance and enforcement

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

Informal requests

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

Formal actions

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

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

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

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

Compliance and enforcement options

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

Outcome	**Formal action** - directed towards end-users	**Formal action** - directed towards online service providers
Put an online service provider on notice		Give one of the following **service provider notifications**: • a written notice informing an online service provider that material that meets the definition of adult cyber abuse is on its service • a statement informing an online service provider that material that meets the definition of adult cyber abuse and that breaches the service's own terms of use is, or was, on its service on two or more occasions over the past 12 months. In addition, eSafety may publish this statement on our website.
Require removal of content	Give a removal notice to an end-user requiring the end-user to take all reasonable steps to remove the material within 24 hours (or longer if allowed by eSafety). This can be given where eSafety has received a valid complaint and eSafety is satisfied a complaint has been made about the material to the relevant online service provider and removal has not occurred within 48 hours.	Give a removal notice to an online service provider requiring the online service provider to take all reasonable steps to remove the material on the service or take all reasonable steps to cease hosting the material within 24 hours (or longer if allowed by eSafety). This can be given where a valid complaint has been received by eSafety and eSafety is satisfied a complaint has been made about the material to the relevant online service provider and removal has not occurred within 48 hours.
Take enforcement action	Options for failing to comply with a removal notice: • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. Failure to comply with a Part 14 notice may also attract certain penalties.	Options for failing to comply with a removal notice: • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. Failure to comply with a Part 13 or Part 14 notice may also attract certain penalties.

Service provider notifications

What are service provider notifications?

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

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

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

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

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

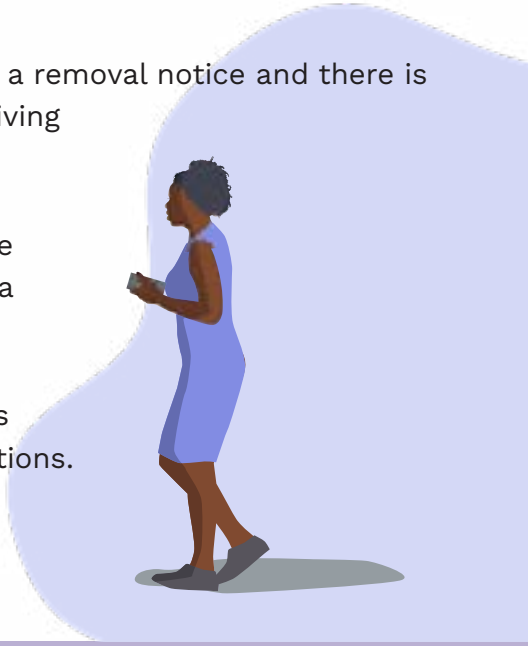
To give this statement, the material must also have breached the service's own terms of use. The purpose of publishing this statement is to call out services that are not doing enough to combat adult cyber abuse.[17] eSafety will generally give an online service provider a chance to comment (and take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

What are the consequences of a service provider notification?

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

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

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



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

Removal notices

What is a removal notice?

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

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

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

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

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

- eSafety has received a complaint about adult cyber abuse material
- the adult cyber abuse material has been provided on a social media service, relevant electronic service, designated internet service
- the adult cyber abuse material was the subject of a complaint made to the provider of the service
- the material was not removed from the service within 48 hours after the complaint was made or such longer period as eSafety allows
- eSafety is satisfied that the material is or was adult cyber abuse material targeted at an Australian, and
- the material can be identified in a way that enables the online service provider or end-user to comply with the notice such as for example through screenshots, URLs, usernames or time stamps.[21]

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

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

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

What are the consequences of a removal notice?

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

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

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

Taking enforcement action

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

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

Enforcement options available include the following:

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

Review rights

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

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

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

Basic Online Safety Expectations

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

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

Find more information and support

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

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

Published: December 2023 (Updated)