

s 22 28/02 11:19 am

s 22: Hi s 22 - s 47F will make a report - even if no action can be taken for the additional support. s 47F (s 47F is the additional person who was in that shot)

28/02 11:19 am

Hi s 22 ok thanks for that mate. I won't send you a hypothetical assessment in that case

Thursday, 29 February

s 22 29/02 9:28 am

s 22: sorry to email so latew s 22 Did s 47F lodge a report.

29/02 9:29 am

Sorry s 22 could you remind me of the name? I deleted your email and now it's slipped my mind

29/02 9:29 am

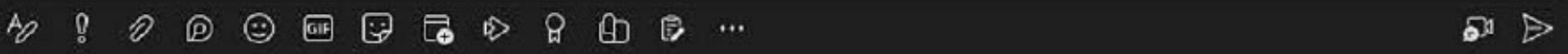
Nothing from s 47F mate

s 22 29/02 9:30 am

s 22: s 47F maybe he is waiting to hear what they come back with



Type a message



OFFICIAL

eSafety FOI 24123
Document 8/59

Hi s 22

So, our IRCT classifies it as refused classification (RC1(a)). s 47E(d) We would encourage the complainant to report the content directly to the platform.

Hope that helps.

From: Cyber Abuse <cyberabuse@esafety.gov.au>
Sent: Thursday, February 29, 2024 12:16 PM
To: s 22 @eSafety.gov.au
Subject: [SEC=OFFICIAL:Sensitive] CRM:0100536

Hi s 22

Second post for your review and advice:
<https://twitter.com/BillboardChris/status/1762620001696244063>

Thanks,
s 22

----- Original Message -----

From: CA Escalations

Received: Fri Mar 01 2024 15:44:37 GMT+1100 (Australian Eastern Daylight Time)

To: Twitter

Subject: Complaint alert for cyber abuse report - NOT-2024-00220 [SEC=OFFICIAL:Sensitive] CRM:0100541

Dear X Corp,

Under the *Online Safety Act 2021*, the eSafety Commissioner is responsible for handling complaints about cyber abuse material concerning Australian adults and ensuring the rapid removal of such material from social media services, relevant electronic services, or designated internet services. Please refer to our website for more information on our role: <https://www.esafety.gov.au/about-the-office>

We wish to alert you to a complaint we have recently received. The eSafety complaint number is NOT-2024-00220. We are alerting this complaint to you on the basis that the material may be in violation of your policies.

s 47F

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

From the information provided in the complaint, the tweets may violate the X Rules and policies. According to the Twitters Rules:

- 'Hateful conduct: You may not directly attack other people on the basis of race, ethnicity, national origin, caste, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.'
- 'Hateful conduct: We prohibit targeting others with repeated slurs, tropes or other content that intends to degrade or reinforce negative or harmful stereotypes about a protected category.'
- 'Sensitive media: Media depicting Gratuitous Gore, Violent Sexual Conduct, or Bestiality and Necrophilia is not permitted.'

We would appreciate your confirmation that you have received this email. We ask that you also advise what actions are taken as a result of this report.

As you are aware, the material may also have been shared or posted elsewhere on your service and we would be grateful for your consideration of any such material and any help you can offer in this regard.

Regards,

Cyber Abuse Team
The eSafety Commissioner

W www.esafety.gov.au



s 22

1/03 3:57 pm

s 22


do you need to see response to s 47F ?

The following Complaint Alert record is now overdue for a response:

eSafety FOI 24123
Document 12/59

- Reference: NOT-2024-00220
- Date Sent: 1/03/2024 3:44 PM
- Due Date: 2/03/2024 3:44 PM
- Record URL: <https://case.crme.case.mgmt.local.443/main.aspx?etc=10124&id=81cbc4c5-84d7-ee11-a320-0050569455e4&histKey=114830645&newWindow=true&pagetype=entityrecord>

You don't often get email from support@twitter.com. [Learn why this is important.](#)

eSafety FOI 24123
Document 13/59 

Hello,


Thank you for your report. Our team is now investigating this matter. We appreciate your patience, cooperation, and will follow up as soon as possible.

Thanks,

Twitter

[Help](#) | [Privacy](#)

X Corp. 1355 Market Street, Suite 900 San Francisco, CA 94103

eSafety FOI 24123 
Document 14/59

Hello,


We have received your request and will get back to you as soon as possible. Thanks for your patience!

X Support

2024-03-01 04:44

ref:00DA0000000K0A8.500Vp000003aAQZ:ref

You don't often get email from support@twitter.com. [Learn why this is important](#)

eSafety FOI 24123 
Document 15/59

This is an AUTOMATED response from our support system.

Hello,

This automated response confirms receipt of your request to Twitter to remove content regarding user(s) @BillboardChris (first user identified in your request).

Your request has been escalated to the appropriate team and will be reviewed and responded to as soon as possible. Please refrain from submitting duplicate requests as this may slow down the assessment of your original request.

We will contact you at the law enforcement / government email address you have provided should we require more information. If you have more information to provide or if the situation has changed, please reply directly to this email. Please include all information in the body of your email, as our system removes attachments for security purposes..


Thanks,

Twitter

Your case number: #0363820601

ref:00DA0000000K0A8.500Vp000004L10m:ref

You don't often get email from support@twitter.com. [Learn why this is important](#)

eSafety FOI 24123 
Document 16/59

Hello,

Thanks once again for your request. We are looking into this request, as a matter of priority. We appreciate your patience, cooperation. We will follow up on this as soon as possible.

Thanks,

X

[Help](#) | [Privacy](#)

X Corp. 1355 Market Street, Suite 900 San Francisco, CA 94103

----- Original Message -----

From: Twitter

Received: Wed Mar 06 2024 04:26:10 GMT+1100 (Australian Eastern Daylight Time)

To: CA Escalations

Subject: Case# 0361920761: Complaint alert for cyber abuse report - NOT-2024-00220 [SEC=OFFICIAL:Sensitive]
CRM:0100541 [ref:!00DA00K0A8.!500Vp03aAQZ:ref]



Hello,

Thanks for reaching out. We reviewed the reported content, and didn't find it to be in violation of the [Twitter rules](#). In this case, no action will be taken at this time.

If you have further concerns about intellectual property, your privacy, or your personal safety, the following guidelines can be of assistance:

Intellectual property

- Report any [copyright infringement](#) by using our [intellectual property issues form](#).
- If the content is hosted on a third-party website, make sure to contact that website's support team to report it.

Privacy & non-consensual nudity

Report violations of your privacy, including any images or videos that depict you without your permission by using our [private information form](#).

Personal safety

- If you feel that you're in danger, we recommend contacting your local law enforcement as soon as possible.
- Take screenshots and document any Tweets that you believe indicate a threat.
- Law enforcement authorities should review our [law enforcement guidelines](#) when seeking information about a Twitter account.

If you have new information that you feel is important to this investigation, please reply to this email with as much detail as you can. We appreciate your help, and hope you'll continue to report anything that you believe may violate our rules and policies.

Thank you,

Twitter

[Help](#) | [Privacy](#)

X Corp. 1355 Market Street, Suite 900 San Francisco, CA 94103



ref:!00DA00K0A8.!500Vp03aAQZ:ref

Complaint alert to be sent to X via X's online portal under Section 88 of the Online Safety Act 2021

Administrative

- eSafety references: ACA-2024-0496095 / NOT-2024-00220
- The X post is available at: <https://twitter.com/BillboardChris/status/1762620001696244063>
- The end user is @BillboardChris.
- The "legal basis" for the removal request will be s 88 of the *Online Safety Act*.
- The "Issue type" will be nominated as "Hateful conduct".

Substance

(This will be inserted in the "Please provide any additional details" section.)

eSafety reference: NOT-2024-00220

The X post is available at: <https://twitter.com/BillboardChris/status/1762620001696244063>

s 47E(d), s 47F
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]


[Redacted]

[Redacted]

[Redacted]

[Redacted]

s 47E(d), s 47F



From: § 22
Sent: Wednesday, 13 March 2024 4:04 PM
To: § 22
Subject: RE: For review: s88 & SOR [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi § 22

I have accepted the changes and made a slight amendment to the assessment section of the Removal Notice.

Thanks,

§

From: § 22 @esafety.gov.au>
Sent: Tuesday, March 12, 2024 12:46 PM
To: § 22 @eSafety.gov.au>
Subject: RE: For review: s88 & SOR [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi § 22

I've made changes to the Statement of Reasons. See particularly some of the assessment I have added.

Have a look and let me know if you agree. If so, we will need to make a couple of changes to the Removal Notice.

Thanks

§ 22

From: § 22 @eSafety.gov.au>
Sent: Monday, March 11, 2024 4:16 PM
To: § 22 @esafety.gov.au>
Subject: For review: s88 & SOR [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi § 22

For your review:

 [ACA-2024-0496095 - Statement of Reasons - s88 Removal notice to X Corp.docx](#)

 [ACA-2024-0496095 - Section 88 Removal notice to X Corp.docx](#)

Thanks,

§

From: Cyber Abuse
Sent: Friday, 22 March 2024 10:46 AM
To: § 22
Cc: § 22
Subject: New approval record: APP-2024-0018 CRM:0100601

Hi § 22 ,

Record URL:

<https://case.crme.case.mgmt.local:443/main.aspx?etc=8&id=e2c6ddd2-1321-ee11-a318-0050569455e4&histKey=625601780&newWindow=true&pagetype=entityrecord>

Record Number:

APP-2024-0018

Regarding Record Number:

ACA-2024-0496095

Requested by:

§ 22

Recommended action:

CB/ACA Removal Notice

Details:

s88 notice to X

From: § 22
Sent: Friday, 22 March 2024 11:17 AM
To: § 22
Cc: Cyber Abuse
Subject: RE: LS-324: Review of s 88 notice [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Attachments: ACA-2024-0496095 - Section 88 Statement of Reasons.pdf

**OFFICIAL: Sensitive
Legal Privilege**

Hi §

Find attached signed statement of reasons.

Thanks
§ 22

From: § 22
Sent: Friday, March 22, 2024 10:17 AM
To: § 22 @eSafety.gov.au
Subject: RE: LS-324: Review of s 88 notice [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]

**OFFICIAL: Sensitive
Legal Privilege**

Hi §

Signed s 88 notice attached.

This can now be sent.

Thanks
§ 22

From: § 22 @eSafety.gov.au
Sent: Thursday, March 21, 2024 12:39 PM
To: § 22 @esafety.gov.au
Subject: RE: LS-324: Review of s 88 notice [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]

**OFFICIAL: Sensitive
Legal Privilege**

Hi § 22

I have accepted all but one change (in the Notice) which incorrectly states that the complainant § 47F

The rest of the Notice and SOR looks good to me.

Thanks,

s 22

From: s 22 <[REDACTED]@esafety.gov.au>
Sent: Thursday, March 21, 2024 9:19 AM
To: s 22 <[REDACTED]@eSafety.gov.au>
Subject: FW: LS-324: Review of s 88 notice [SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]

**OFFICIAL: Sensitive
Legal Privilege**

Hi s [REDACTED]

See below and attached from legal.

Can you let me know if you are happy with their changes (and if so accept them), then I will sign.

Thanks

s 22

s 42





22 March 2024

X Corp

Submitted via X's Legal Request submission site: <https://t.co/lr>

Our Reference: ACA-2024-0496095

Removal notice requiring you to remove cyber-abuse material targeted at an Australian adult from your service

(Under section 88 of the *Online Safety Act 2021* (Cth))

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

Please see enclosed a removal notice given to you under section 88 of the Act (**Notice**). The Notice requires you to take all reasonable steps to ensure the removal of the material from your service within **24 hours** of being given the Notice.

Background

On 29 February 2024, the eSafety Commissioner received a complaint under section 36 of the Act (**the Complaint**) about cyber abuse material targeted at an Australian adult that is available on a service that you provide (**the Material**).

s 47E(d), s 47F



s 47E(d), s 47F

I am satisfied that:

- a) the Material is provided on a social media service;
- b) the Material was the subject of a complaint that was made to the provider of the service;
- c) the Material was not removed from the service within 48 hours after the complaint was made, or within a longer period that was allowed by the eSafety Commissioner;
- d) a complaint has been made to the eSafety Commissioner under section 36 of the Act about the Material; and
- e) the Material is cyber-abuse material targeted at an Australian adult within the meaning of the Act.

On this basis, I have decided to give you the Notice.

Required action

Please email requests@esafety.gov.au once you have taken all reasonable steps to ensure the removal of the Material in compliance with the Notice. Failure to comply with the Notice may result in compliance or enforcement action being taken against you without further notice.

If you have any questions about the Notice or if you require a longer period of time to comply, contact our office by email to requests@esafety.gov.au as soon as you receive this Notice.

Failure to comply

Under section 91 of the Act, you must comply with a requirement under a removal notice given under section 88 of the Act to the extent that you are capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of \$782,500 (AUD) for a single contravention by a body corporate.

Review rights

You have a right to seek an internal or external review of the decision to give you a removal notice.

An internal review is a review conducted by the eSafety Commissioner under the Internal Review Scheme. There is no fee associated with a request for an internal review.



An external review is a review conducted by the Administrative Appeals Tribunal (**AAT**). The enclosed information sheet sets out your rights regarding the different review options available to you, as well as other options if you do not agree that the Notice should have been given to you.

Please note that you are required to comply with the Notice even if you have made an application for internal or external review, unless you receive notice that the eSafety Commissioner or the AAT has decided otherwise.

Manager, Adult Cyber Abuse Section (EL2)
Delegate of the eSafety Commissioner

Enclosed: Notice under section 88 of the Act

Information Sheet



REMOVAL NOTICE TO REMOVE CYBER-ABUSE MATERIAL FROM YOUR SERVICE

Under section 88 of the *Online Safety Act 2021* (Cth)

To: X Corp

Submitted via X's Legal Request submission site: <https://t.co/lr>

I am a delegate of the eSafety Commissioner for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).

This removal notice is given to you under section 88 of the Act and requires you to take all reasonable steps to ensure the removal of the material from your service specified in **Schedule A**.

You are required to comply with this requirement within **24 hours** of being given this notice, or within such longer period as I allow if contacted by you with a request for an extension.

Section 91 of the Act provides that a person must comply with a requirement under a removal notice given under section 88 of the Act to the extent that the person is capable of doing so.

Failure to comply with the Notice may result in enforcement action, including the commencement of civil penalty proceedings for a civil penalty order of up to a maximum penalty of \$782,500 (AUD) for a single contravention by a body corporate.

Date: 22 March 2024

s 22

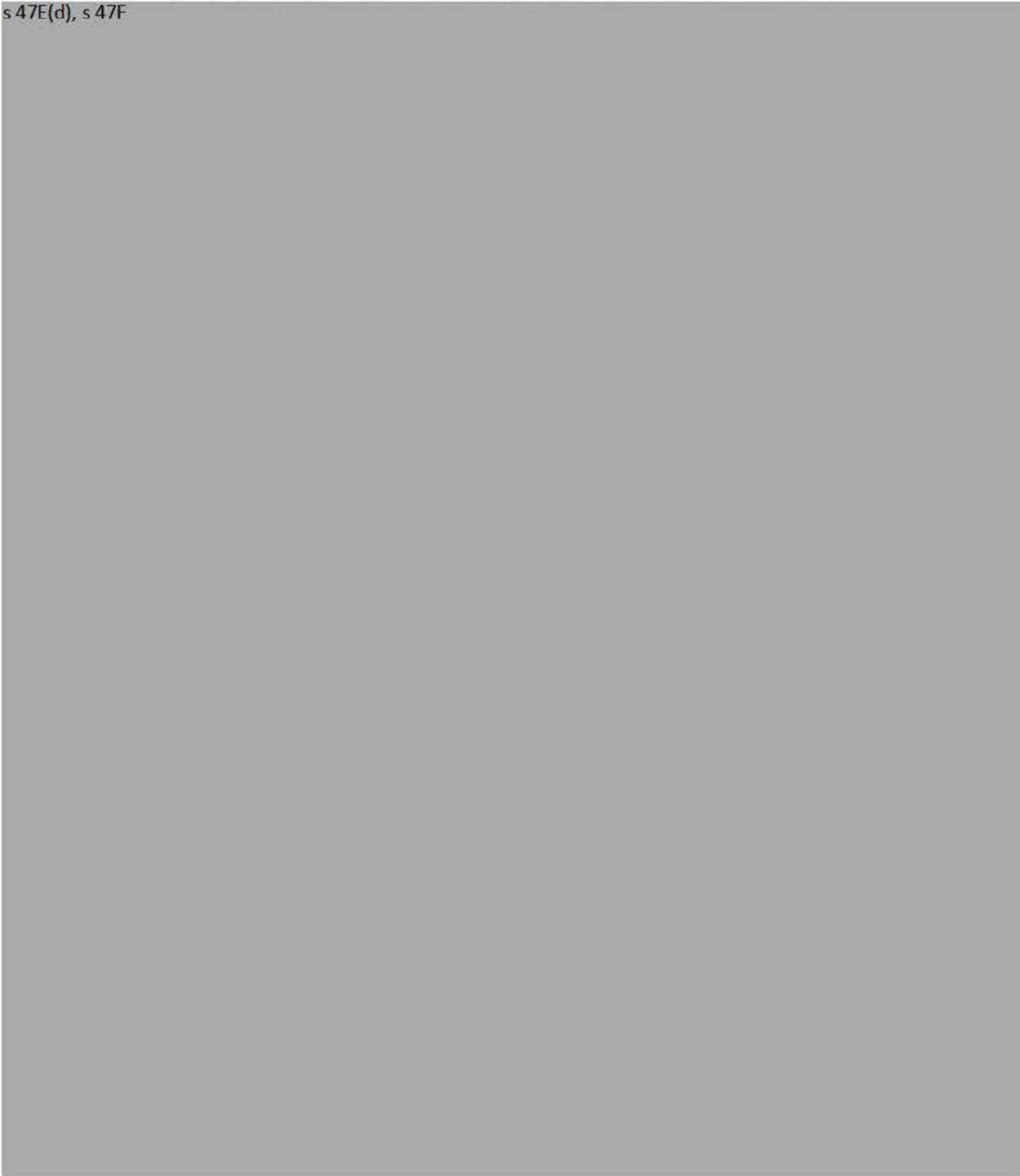
**Manager, Adult Cyber Abuse (EL2)
Delegate of the eSafety Commissioner**



Schedule A – The Material for removal

<https://twitter.com/BillboardChris/status/1762620001696244063>

s 47E(d), s 47F

A large, solid grey rectangular box covers the majority of the page, indicating that the content has been redacted.



Statement of Reasons

Date	22 March 2024
Decision	To give the attached removal notice to X Corp, under section 88 of the <i>Online Safety Act 2021</i> (Cth)
Decision-maker	Acting Manager, Adult Cyber Abuse
Case reference	ACA-2024-0496095

Introduction

1. I am a delegate of the eSafety Commissioner (eSafety) for the purposes of section 88 of the *Online Safety Act 2021* (Cth) (**the Act**).
2. This statement sets out my reasons to give the attached removal notice to X Corp under section 88 of the Act (**the Notice**). The Notice requires X Corp to take all reasonable steps to ensure the removal of the material specified in the notice as cyber-abuse material targeted at an Australian adult (**the Material**).

Legislative framework

3. Part 7 of the Act establishes a scheme for the removal of cyber-abuse material targeted at an Australian adult from a social media service, relevant electronic service, designated internet service and hosting service.
4. Section 88 provides eSafety with the power, if certain requirements are met, to give a removal notice to a provider of a social media service, relevant electronic service or designated internet service requiring them to take all reasonable steps to remove adult cyber-abuse material from the service.

Decision


5. I have decided to give the Notice to X Corp under section 88 of the Act based on the Material and the reasons below.

Material relied upon to make decision


6. I have taken the following information into account in making my decision:
 - a. The complaint made under section 36(1) of the Act by **the eSafety Complainant**.
 - b. The following information ascertained by eSafety in handling the eSafety Complainant:
 - i. On 28 February 2024, the Complainant made a report to X Corp (**the Provider Complainant**).

- ii. On 29 February 2024 at 11:35am, eSafety received the eSafety Complaint.

s 47E(d), s 47F



s 47E(d), s 47F



7. I have taken the following documents into account in making my decision:
 - a. The Material, as described above and attached at **Appendix B**;
 - b. eSafety's Adult Cyber Abuse Scheme Regulatory Guidance (December 2023); and
 - c. The relevant sections of the Act which are extracted in **Appendix A**.


Reasons for decision

8. I am satisfied that the requirements for giving a removal notice under section 88 of the Act have been met. Having considered the above documents and information, I am satisfied that:
 - a. The Material is provided on X Corp's X service, which is a social media service, within the meaning of section 13 of the Act. This is because X is an electronic service that has the sole or primary purpose of enabling online social interaction between two or more end-users, allows end-users to link to and interact with other end-users, and allows end-users to post material to the service.
 - b. The Material is provided on the service within the meaning of section 10 of the Act because the Material is accessible to, or delivered to, one or more other end-users using the service through a hyperlink or URL that is accessible to the public (<https://twitter.com/BillboardChris/status/1762620001696244063>).
 - c. The Material was the subject of the Provider Complaint, which was made to the provider of the service. The Complainant submitted a report to X Corp about the Material on 28 February 2024. A screenshot of the Provider Complaint was provided to eSafety on 8 March 2024 (see Appendix C).
 - d. The Material the subject of the Provider Complaint was not removed from the service within 48 hours of the Provider Complaint.
 - e. On 1 March 2024, eSafety sent an informal complaint alert to X Corp via email at AUEScalations@twitter.com. On 6 March 2024, X Corp responded to eSafety's request. X Corp informed eSafety that they reviewed the reported

content and did not find it to be in violation of their policies. They stated that because of that decision, no action would be taken.

f. The Material is available at the same location on the service to date.

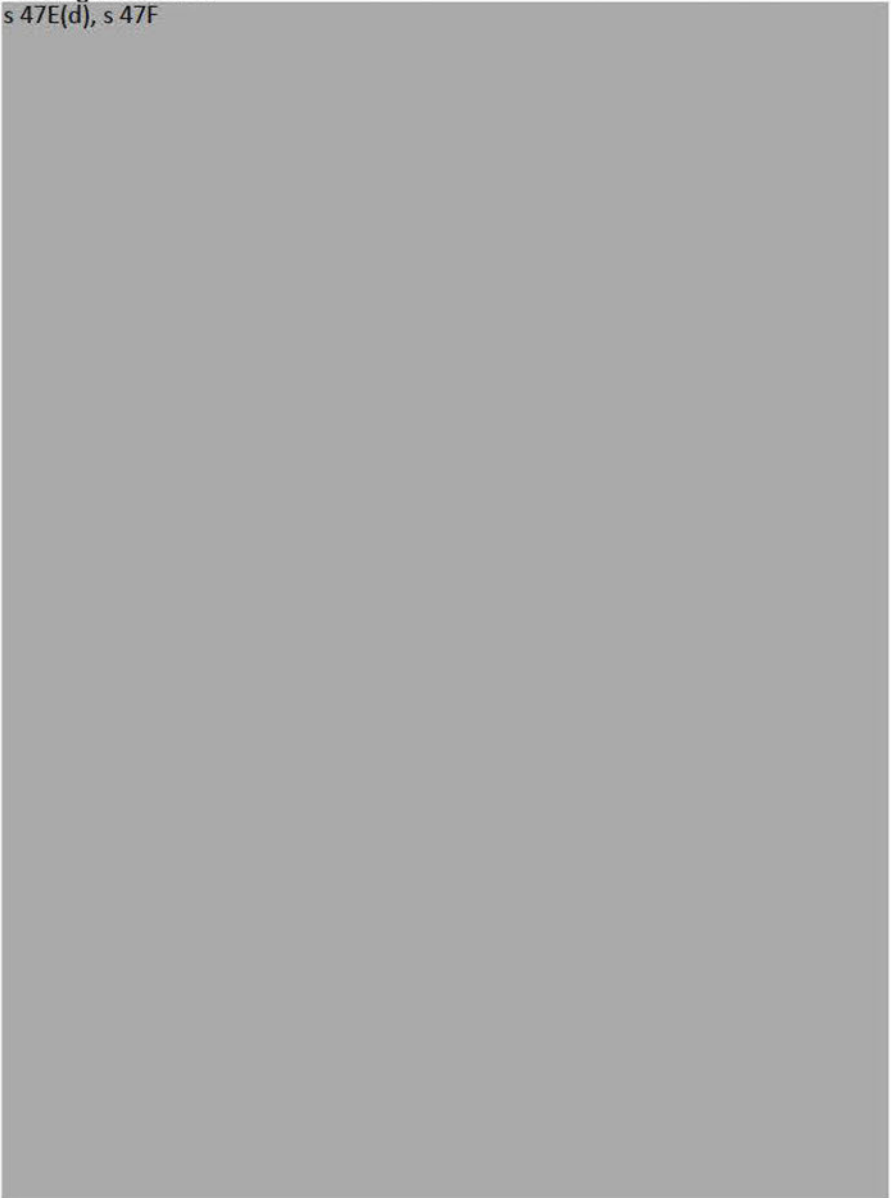
s 47E(d), s 47F



h. The Material is cyber-abuse material targeted at an Australian adult within the meaning of section 7 of the Act because:

- i. The Material is provided on a social media service.
- ii. An ordinary reasonable person would conclude that it is likely that the Material was intended to have an effect of causing 'serious harm', as defined in section 5 of the Act, to a particular Australian adult based on the following reasons:

s 47E(d), s 47F



s 47E(d), s 47F



iii. An ordinary reasonable person in the position of the Australian adult would regard the Material as being, in all the circumstances, offensive based on the following:

- o The Material exceed the standards of morality, decency and propriety generally accepted by reasonable adults. Although, it is understood that society permits a degree of online disagreement, particularly where it relates to political or topical concerns, s 47E(d), s 47F



The Material therefore does not meet these standards;

- o The Material does not have any apparent literary, artistic or educational merit;
- o The Material is in the character of a social media post, and is not of medical, legal or scientific character; and
- o I consider that while an ordinary reasonable person would consider the Material offensive regardless of whether s



Conclusion

The reasons provided above are the reasons for my decision to give the Notice under section 88 of the Act to X Corp.

Signed:

s 22



Manager, Adult Cyber Abuse Section (EL2)
Delegate of the eSafety Commissioner

Date: 22 March 2024

Appendix A – Extracts of relevant sections of the *Online Safety Act 2021 (Cth)*

7 Cyber-abuse material targeted at an Australian adult

- (1) For the purposes of this Act, if material satisfies the following conditions:
- (a) the material is provided on:
 - (i) a social media service; or
 - (ii) a relevant electronic service; or
 - (iii) a designated internet service;
 - (b) an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult;
 - (c) an ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive;
 - (d) such other conditions (if any) as are set out in the legislative rules;
- then:
- (e) the material is ***cyber-abuse material targeted at the Australian adult***, and
 - (f) the Australian adult is the ***target*** of the material.

Note: For ***serious harm***, see section 5.

- (2) An effect mentioned in paragraph (1)(b) may be:
- (a) a direct result of the material being accessed by, or delivered to, the Australian adult; or
 - (b) an indirect result of the material being accessed by, or delivered to, one or more other persons.

8 Determining whether material is offensive

(1) The matters to be taken into account in deciding for the purposes of this Act whether an ordinary reasonable person in the position of a particular Australian adult would regard particular material as being, in all the circumstances, offensive, include:

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

(2) If:

- (a) material is provided on:
 - (i) a social media service; or
 - (ii) a relevant electronic service; or
 - (iii) a designated internet service; and
- (b) the material is private sexual material;

then, in deciding for the purposes of this Act whether an ordinary reasonable person in the position of a particular Australian adult would regard the material

as being, in all the circumstances, offensive, regard must be had to whether the subject, or each of the subjects, of the private sexual material gave consent to the material being provided on the service.

(3) Subsection (2) does not limit subsection (1).

36 Complaints about cyber-abuse material

Complaint made by an Australian adult

- (1) If an Australian adult has reason to believe that the adult was or is the target of cyber-abuse material that has been, or is being, provided on:
- (a) a particular social media service; or
 - (b) a particular relevant electronic service; or
 - (c) a particular designated internet service;
- the adult may make a complaint to the Commissioner about the matter.

Complaint made on behalf of an Australian adult

- (2) If:
- (a) a person (the **responsible person**) has reason to believe that cyber-abuse material targeted at an Australian adult has been, or is being, provided on:
 - (i) a particular social media service; or
 - (ii) a particular relevant electronic service; or
 - (iii) a particular designated internet service; and
 - (b) the adult has authorised the responsible person to make a complaint about the matter;
- the responsible person may, on behalf of the adult, make a complaint to the Commissioner about the matter.

Complaint about material that was provided on a service

- (3) If:
- (a) a complaint made by a person under this section concerns material that has been, or is being, provided on:
 - (i) a social media service; or
 - (ii) a relevant electronic service; or
 - (iii) a designated internet service; and
 - (b) the person wants the Commissioner to give the provider of the service a removal notice under section 88 requiring the provider to remove the material from the service;
- the complaint under this section must be accompanied by evidence that the material was the subject of a complaint that was previously made to the provider of the service.
- (4) For the purposes of subsection (3), evidence must be in a form required by the Commissioner.
- (5) If:
- (a) a social media service; or
 - (b) a relevant electronic service; or
 - (c) a designated internet service;

issues a receipt or complaint number to a complainant as part of its ordinary business processes, the Commissioner may require evidence to be in the form of the receipt or complaint number.

- (6) If:
- (a) a social media service; or
 - (b) a relevant electronic service; or
 - (c) a designated internet service;
- does not issue a receipt or complaint number to a complainant as part of its ordinary business processes, the Commissioner may require evidence to be:
- (d) in the form of a screen shot; or
 - (e) in the form of a statutory declaration; or
 - (f) in such other form as the Commissioner specifies.
- (7) Subsections (5) and (6) do not limit subsection (4).
- (8) A requirement under subsection (4), (5) or (6) is not a legislative instrument.

88 Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

- (1) If:
- (a) material is, or has been, provided on:
 - (i) a social media service; or
 - (ii) a relevant electronic service; or
 - (iii) a designated internet service; and
 - (b) the Commissioner is satisfied that the material is or was cyber-abuse material targeted at an Australian adult; and
 - (c) the material was the subject of a complaint that was made to the provider of the service; and
 - (d) if such a complaint was made—the material was not removed from the service within:
 - (i) 48 hours after the complaint was made; or
 - (ii) such longer period as the Commissioner allows; and
 - (e) a complaint has been made to the Commissioner under section 36 about the material;
- the Commissioner may give the provider of the service a written notice, to be known as a **removal notice**, requiring the provider to:
- (f) take all reasonable steps to ensure the removal of the material from the service; and
 - (g) do so within:
 - (i) 24 hours after the notice was given to the provider; or
 - (ii) such longer period as the Commissioner allows.
- (2) So far as is reasonably practicable, the material must be identified in the removal notice in a way that is sufficient to enable the provider of the service to comply with the notice.

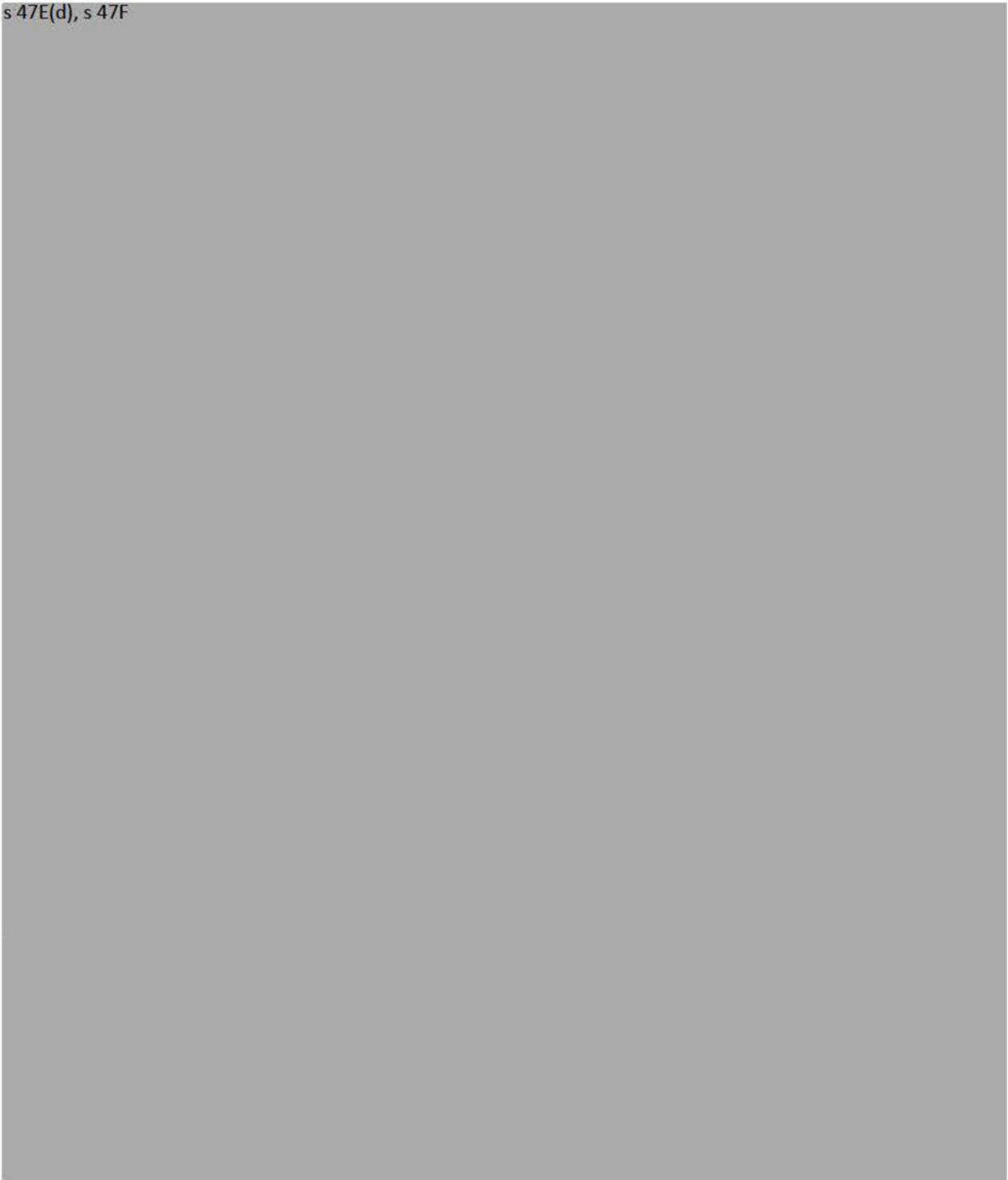
Notice of refusal to give a removal notice

- (3) If the Commissioner decides to refuse to give a removal notice under subsection (1), the Commissioner must give written notice of the refusal to the person who made the complaint to the Commissioner under section 36.

Appendix B – the Material the subject of the Notice

<https://twitter.com/BillboardChris/status/1762620001696244063>

s 47E(d), s 47F



Appendix C – the Provider Complaint


×

Report - February 28, 2024

You submitted a report for hateful conduct

[View Rule](#)

s 47E(d), s 47F



What's next

Our team and technology will review your report. If we find a rule violation, we'll let you know what actions we're taking.

What's our process?

Context matters. We consider the following factors when enforcing our rules (this isn't a complete list):

- Does the reported content target people because of their identity?
- How severe is this violation?
- Was the report submitted by the person being targeted?

Creating duplicate reports will not accelerate our process.

Record URL:

<https://case.crime.case.mgmt.local:443/main.aspx?etc=10075&id=f115f126-dde7-ee11-a320-0050569455e4&histKey=423365448&newWindow=true&pagetype=entityrecord>

Record number:

APP-2024-0018

Approving user:

11/15/22

Approval to proceed:

Yes

Approval date:

22/03/2024

Approval comment:

Approving this s 88 notice to be sent to X/Twitter.

Regulatory Notice Record URL:

<https://case.crime.case.mgmt.local:443/main.aspx?etc=10124&id=4e737a9f-dde7-ee11-a320-0050569455e4&histKey=423365448&newWindow=true&pagetype=entityrecord>

----- Original Message -----

From: no-reply@twitter.com

Received: Fri Mar 22 2024 12:22:25 GMT+1100 (Australian Eastern Daylight Time)

To: Requests

Subject: Access link to Twitter legal request submission system

Hello,

This is an automated response. Please do not reply to this email as it will not be received by our system.

We have received your request to access our online legal request submission system. Please use the following unique link to log into our secure site where you will be able to submit your legal request:

https://legalrequests.twitter.com/forms/access_disclaimer/pwA1quM3QL9NkOba2NWfAWt1jxMHKESJWilvwkn0d%2FE%3D

Access via this unique link will expire on March 22, 2024 at 2:22AM UTC. Should you need to request a new link, please return to our secure site:

<https://legalrequests.twitter.com>

For other questions, please review our Guidelines for Law Enforcement:

<https://t.co/le>

NOTE: Twitter reserves the right to pursue legal remedies against unauthorized access to this system.

Sincerely,
Twitter

From: § 22
Sent: Monday, 25 March 2024 2:50 PM
To: § 47F @twitter.com
Cc: Cyber Abuse
Subject: Removal Notice - NOT-2024-00345 [SEC=OFFICIAL:Sensitive]
Attachments: ACA-2024-0496095 - Section 88 Removal notice to X Corp.pdf

OFFICIAL: Sensitive

Dear § 47F

On 22 March, eSafety sent X a Removal Notice under section 88 of the *Online Safety Act 2021*.

That Notice related to the following post, which remains online:
<https://twitter.com/BillboardChris/status/1762620001696244063>.

We have attached the notice for your reference. As you will see, X were required to take all reasonable steps to ensure the removal of the material within 24 hours of being given the Notice.

On 22 March at 2.06pm (AEDT), eSafety received an email from X advising, amongst other things, that: "Our team is now investigating the matter."

To date, we have not received any further correspondence from X. I am writing to follow this up on your end, as we are now at about the 72-hour mark since X was given the Notice.

§ 22
Manager (A/g) – Adult Cyber Abuse | Investigations



 eSafety Commissioner



eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.

----- Original Message -----

From: Twitter

Received: Tue Mar 26 2024 10:00:49 GMT+1100 (Australian Eastern Daylight Time)

To: Requests

Subject: Case# 0363820601: Twitter Receipt of Content Removal Request - Office of the eSafety Commissioner [ref:!00DA00K0A8.!500Vp04L10m:ref]

You don't often get email from support@twitter.com. [Learn why this is important](#)



Hello,

The following reported content has been withheld in Australia

<https://x.com/BillboardChris/status/1762620001696244063>

Thanks,

X

[Help](#) | [Privacy](#)

X Corp. 1355 Market Street, Suite 900 San Francisco, CA 94103



ref:!00DA00K0A8.!500Vp04L10m:ref

----- Original Message -----

From: s 47F
Received: Tue Mar 26 2024 12:22:33 GMT+1100 (Australian Eastern Daylight Time)
To: s 22
Cc: Cyber Abuse; Cyber Abuse
Subject: Re: Removal Notice - NOT-2024-00345 [SEC=OFFICIAL:Sensitive]

You don't often get email from s 47F@x.com. [Learn why this is important.](#)

Hi s 22

An update: After additional reviews our teams responded directly in-channel.

Please don't hesitate to let us know if you have further questions, or if it would be helpful to connect.

Kind regards,

s 47F

On Mon, 25 Mar 2024 at 13:19, s 47F <[redacted]@x.com> wrote:

Hi s 22

Thank you. Acknowledging here. Confirming teams are across this case and have sent a follow up response in the interim as well. Please let me know if you have any questions.

Kind regards,

On Mon, Mar 25, 2024 at 12:49 PM s 22 <[redacted]@esafety.gov.au> wrote:

OFFICIAL: Sensitive

Dear s 47F

On 22 March, eSafety sent X a Removal Notice under section 88 of the *Online Safety Act 2021*.

That Notice related to the following post, which remains online:
<https://twitter.com/BillboardChris/status/1762620001696244063>.

We have attached the notice for your reference. As you will see, X were required to take all reasonable steps to ensure the removal of the material within **24 hours** of being given the Notice.

On 22 March at 2.06pm (AEDT), eSafety received an email from X advising, amongst other things, that: “Our team is now investigating the matter.”

To date, we have not received any further correspondence from X. I am writing to follow this up on your end, as we are now at about the 72-hour mark since X was given the Notice.

s 22

Manager (A/g) – Adult Cyber Abuse | Investigations



eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.



----- Original Message -----

From: s 22 [@esafety.gov.au](mailto:s22@esafety.gov.au)

Received: Tue Mar 26 2024 12:39:24 GMT+1100 (Australian Eastern Daylight Time)

To: Cyber Abuse; Cyber Abuse

Cc: s 22 Media OeSC

Subject: ATTN: Social media post re: notice ACA2024-0496095 [SEC=OFFICIAL]

OFFICIAL

Hi team, hope you're well. We've seen the attached post from [Billboard Chris](#), which is regarding a recent notice ES sent to X to take down the offending Tweet.



We wanted to let you know, as this person has a sizeable following (396.5K people) and an active presence on Twitter/X.

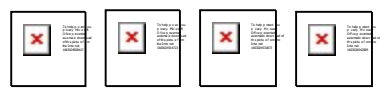
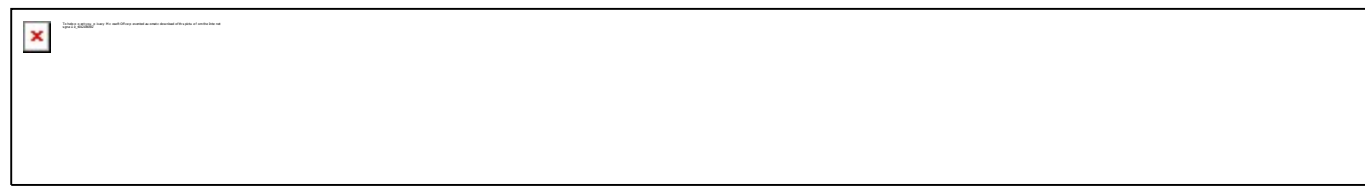
We won't be taking any action unless requested, as the original Tweet has already been removed (see 3rd screenshot).

Thanks,

s 22


Social Media and Digital Content Producer

 s 22 



eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.

From: s 22
Sent: Tuesday, 26 March 2024 1:29 PM
To: s 22
Subject: RE: ATTN: Social media post re: notice ACA2024-0496095 CRM:0127690 [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Sorry – nevermind, I see you already sent it – my bad!

From: s 22
Sent: Tuesday, March 26, 2024 1:28 PM
To: s 22 <s22@esafety.gov.au>
Subject: RE: ATTN: Social media post re: notice ACA2024-0496095 CRM:0127690 [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s 22

Can you please send through the attachment that s 22 sent through? I assume the post re our notice is not geoblocked but I couldn't see it when I looked at the x account.

Thanks

s

From: s 22 <s22@esafety.gov.au>
Sent: Tuesday, March 26, 2024 1:01 PM
To: s 22 <s22@esafety.gov.au>
Cc: Cyber Abuse <cyberabuse@esafety.gov.au>; s 22 <s22@eSafety.gov.au>; s 22 <s22@esafety.gov.au>; s 22 <s22@eSafety.gov.au>; Media OeSC <media@esafety.gov.au>; s 22 <s22@eSafety.gov.au>
Subject: RE: ATTN: Social media post re: notice ACA2024-0496095 CRM:0127690 [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s 22

Thanks for this. I have also CC'ed in s 22 and s 22 for situational awareness.

The material has not actually been removed. It has been "geo-blocked", which means that X users in Australia will not be able to see it.

Users elsewhere, however, or those using a VPN, can still see the material.

Kind regards

s 22
Manager (A/g) – Adult Cyber Abuse | Investigations



eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.

----- Original Message -----

From: s 22 [@esafety.gov.au](mailto:s22@esafety.gov.au)
Received: Tue Mar 26 2024 12:39:24 GMT+1100 (Australian Eastern Daylight Time)
To: Cyber Abuse; Cyber Abuse
Cc: s 22 ; s 22 ; Media OeSC
Subject: ATTN: Social media post re: notice ACA2024-0496095 [SEC=OFFICIAL]

OFFICIAL

Hi team, hope you're well. We've seen the attached post from [Billboard Chris](#), which is regarding a recent notice ES sent to X to take down the offending Tweet.

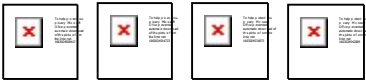
We wanted to let you know, as this person has a sizeable following (396.5K people) and an active presence on Twitter/X.

We won't be taking any action unless requested, as the original Tweet has already been removed (see 3rd screenshot).

Thanks,
s 22


Social Media and Digital Content Producer

 s 22



eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters and community. We pay our respects to First Nations people, and to Elders past, present and future.



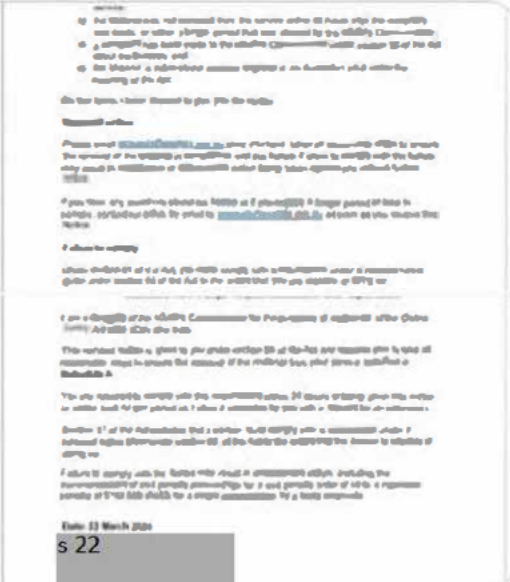
The Australian government has ordered my tweet below to be taken down. @X can face a fine of up to \$782,500 AUD if they do not comply.

I don't know if any civil action or fine can be directed at me under that law.

A delegate for the eSafety Commissioner says "an ordinary...

[x.com/billboardchris...](#)

Show more



This post is unavailable.

15

38

97

7



Post your reply

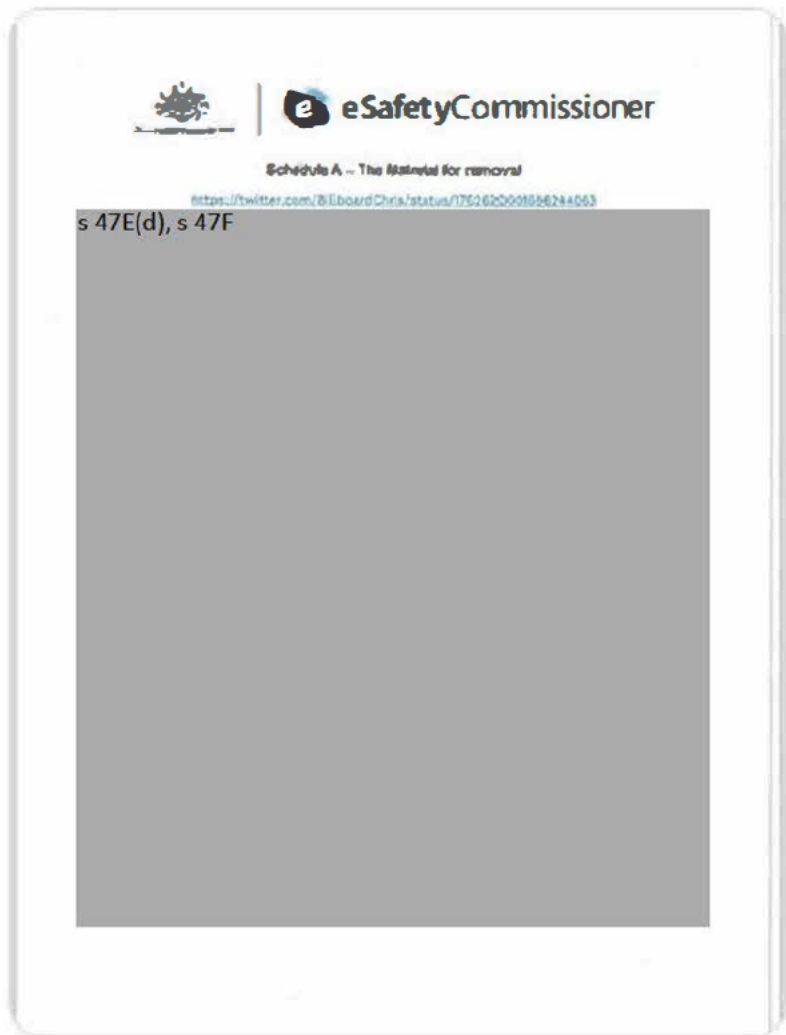
Reply



Billboard Chris 🇨🇦 🇺🇸 ✓ @BillboardChris · 5m



Here's the last page of the Australian government's correspondence.



1

6

25

833



eSafety FOI 24123

Document 35/59

s 22 [redacted] 26/03 10:03 am

s 22 [redacted]

s 22 [redacted]

- X has geoblocked the post re s 47F [redacted] matter @

E-MAIL: INFORMATION
New adult cyber abuse complaint: ACA-2024-...

Owner: [Redacted] 22
Date Sent/Received: 29/02/2024 11:30 AM

E-mail

From: noreply
 To: Cyber Abuse; Cyber Abuse
 Cc: --
 Subject: New adult cyber abuse complaint: ACA-2024-0496095 [SEC=OFFICIAL:Sensitive]
 Classification: [SEC=OFFICIAL:Sensitive]
 Regarding: ACA-2024-0496095

The email below might contain script or content that is potentially harmful and has been blocked. See the full content.

Receipt number: ACA-2024-0496095.

Attachments

File Name ↑	File Size (Bytes)
Complaint Content.pdf	190,407

Status Reason: Received

Activity Status: Received

Read only

APPROVAL: INFORMATION CB/ACA Removal Notice. Approved (22/03/20...

Offline Approval	Recommending User s 22	Approving User s 22	Activity Status Completed
------------------	---------------------------	------------------------	------------------------------

General

Regarding *
ACA-2024-0496095

Recipient	
Platform/Provider	End User
Twitter	--

Recommendation		
Recommending User*	Recommended Action*	Recommendation Date*
s 22	CB/ACA Removal Notice	22/03/2024

Details +
s88 notice to X

Authorisation	
Approving User*	Designation
s 22	EL2
Approval to proceed	Approval Date
Yes	22/03/2024
Approval Comment	
Approving this s 88 notice to be sent to X/Twitter.	

NOTES

Enter a note

No Notes found.

General

Platform Type
DIS

Platform
Dailymail.co.uk

Platform Name (Unqualified)
--

CB/ACA Complaint
ACA-2024-0496095

Owner
s 22

Notice issued?
No

Complainant appealed decision not to issue notice
No

NOTES
Enter a note
No Notes found.

Platform information

Have you already reported the content?
No

Social Media Username
--

Respondent Username
--

Date Reported
--

Please provide an explanation on why you have not reported the content
--

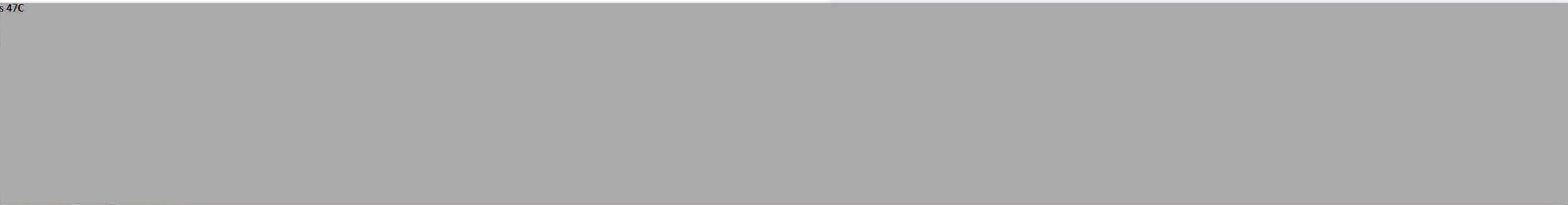
We will need to see evidence that you complained to the platform about cyberbullying material.

Content Still Online?
Yes

Please provide the website URL where we can see the material
--

Do you have the complaint number or reference number from your complaint to the Platform?
No

Receipt number or Complaint number
--



Complaint Categories

Name ↑	Source Type
Defamation	ACA

Username ↑	Platform	Contact	Created On
No Platform Username records found.			

Complained Locators

URL ↑
s 47E[d], s 47F

Related Capture Requests

Number	Capture Ty...	Progress	Complaint alert	Removal Notice	Serious cyberbullying	Serious cyber abuse	Created On ↓
No data available.							

ACTIVITIES NOTES

Enter a note

06/03/2024 0426 - Response from X (0361920761)

"We reviewed the reported content, and didn't find it to be in violation of the Twitter rules. In this case, no action will be taken at this time."

s 22 7/03/2024 10:42 AM

X

01/03/2024 1544 - Informal complaint alert sent to X via email (0361920761)

<https://twitter.com/BillboardChris/status/176262001696244063>

Escalation to X - Hateful conduct & sensitive media - NOT-2024-00220.docx

s 22 1/03/2024 4:06 PM

REGULATORY NOTICE : G3/ACA
 NOT-2024-00220

General

Name
NOT-2024-00220

Owner
 s.22

Record Status
Finalised

Notice Type
Complaint Alert

Type
Informal e.g. ToS breaches

Regarding

Approval
 --

Complaint
 ACA-2024-0496095

Date Sent
1/03/2024 3:44 PM

Method Sent
Email

Due Date
2/03/2024 3:44 PM

Delivery Id
0361920761

ACTIVITIES NOTES

All Add Phone Call Add Task

	Twitter Case# 0361920761: Complaint alert for cyber abuse report - NOT-2024-00220 [SEC=OFFICIAL:Sensitive] CRM:0100541 [ref:00DA00K0A8.1500Vp03aAQZ:ref] 11/03/2024 3:02 PM
	CA Escalations Complaint alert for cyber abuse report - NOT-2024-00220 [SEC=OFFICIAL:Sensitive] CRM:0100541 11/03/2024 3:02 PM
	Cyber Abuse ACTION REQUIRED: Overdue Complaint Alert NOT-2024-00220 CRM:0052286 4/03/2024 1:23 PM
	Cyber Abuse ACTION REQUIRED: Overdue Complaint Alert NOT-2024-00220 CRM:0052286 3/03/2024 8:11 AM

Subjects

Provider 	End User Contact --	School --
--------------	------------------------	--------------

Related Capture Requests

Capture Requests

Number	Capture Ty...	Progress	Complaint alert	Removal Notice	Serious cyberbullying	Serious cyber abuse	Created On
No data available.							

Action(s) and Outcome(s)

Name	Details	Action Date	Outcome	Created On
Complaint alert sent		1/03/2024 3:44 PM	Response received	1/03/2024 3:45 PM
Response received	Material not removed	6/03/2024 4:26 AM	Material not removed	7/03/2024 10:43 AM

Response

Response Received
Yes

Date Response Received
6/03/2024 4:26 AM

Response Time (Hrs)
108.7

Responded within timeframe
No

Removal

Material Removed
 --

Date Material Removed
 --

Notional timeframe for material removal (Hrs)
 --

Material removed within timeframe?
No

Account Removed
No

Date Account Removed
 --

Notional timeframe for account removal (Hrs)
 --

Removal Identified By
 --

Reason Provided for Non-Removal
No violation found by X

Related Complaints

Enter a note

26/03/2024 1000 - Email from X - Material geoblocked

"Hello,

The following reported content has been withheld in Australia

<https://x.com/BillboardChris/status/1762620001696244063>

Thanks,

X"

26/03/2024 1004 - Investigator checked URL, material geoblocked

s 22 - 26/03/2024 11:35 AM

25/03/2024 1907 - Email from X - Pending outcome

×

"Hello,

Thanks once again for your request. We are looking into this request, as a matter of priority. We appreciate your patience, cooperation. We will follow up on this as soon as possible.

Thanks,

X"

s 22 - 26/03/2024 11:34 AM

25/03/2024 - File note - No response from X re formal notice

A/EL2 advised he will follow up with s 47F at X

s 22 - 26/03/2024 11:34 AM

22/03/2024 1235 - Removal notice sent to X via legal request form (0363820601)

<https://twitter.com/BillboardChris/status/1762620001696244063>

s 22 - 22/03/2024 12:39 PM

REGULATORY NOTICE : CB/ACA
NOT-2024-00345

General

Name
 NOT-2024-00345

Owner
 [Redacted]

Record Status
 Finalised

Notice Type
 Removal Notice

Type
 Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Regarding

Approval
 CB/ACA Removal Notice, Approved (22/03/2024)

Complaint
 ACA-2024-0496095

Date Sent
 22/03/2024 12:35 PM

Due Date
 23/03/2024 12:35 PM

Method Sent
 Delivery Id

Provider online form
 0363820601

ACTIVITIES NOTES

All | Add Phone Call | Add Task | ...

Twitter	Case# 0363820601: Twitter Receipt of Content Removal Request - Office of the eSafety Commissioner [ref:!00DA00K0A8.!500Vp04L10m:ref]	28/03/2024 10:38 AM
§ 47F	Re: Removal Notice - NOT-2024-00345 [SEC=OFFICIAL:Sensitive]	26/03/2024 12:55 PM
§ 47F	Re: Removal Notice - NOT-2024-00345 [SEC=OFFICIAL:Sensitive]	26/03/2024 11:36 AM
Twitter	Case# 0363820601: Twitter Receipt of Content Removal Request - Office of the eSafety Commissioner [ref:!00DA00K0A8.!500Vp04L10m:ref]	26/03/2024 11:32 AM

Subjects

Provider Twitter	End User Contact --	School --
----------------------------	-------------------------------	---------------------

Related Capture Requests

Capture Requests

No data available.

Action(s) and Outcome(s)

Name ↑	Details	Action Date	Outcome	Created On
Complaint alert sent	X ref: 0363820601	22/03/2024 12:35 PM	Response received	22/03/2024 12:37 PM
Identified material removed	02/04/2024 - [Redacted] advised that Legal did not provide a ...	26/03/2024 10:00 AM	Identified by platform	3/04/2024 10:03 AM
Response received	Material geoblocked	26/03/2024 10:00 AM	All material removed	26/03/2024 11:35 AM

Response

Response Received
 Yes

Response Time (Hrs)
 93.4

Date Response Received
 26/03/2024 10:00 AM

Responded within timeframe
 No

Removal

Material Removed
 Yes

Notional timeframe for material removal (Hrs)
 93.4

Date Material Removed
 26/03/2024 10:00 AM

Material removed within timeframe?
 No

Account Removed
 No

Date Account Removed
 --

Removal Identified By
 Platform

Reason Provided for Non-Removal
 --

Compliance

Complied with notice?
 Yes

Related Complaints

Active

Twitter

General

Platform Type **SMS**

Platform **Twitter**

Platform Name (Unqualified) **--**

CB/ACA Complaint **ACA-2024-0496095**

Owner **s 22**

Notice issued? **Yes**

NOTES

Enter a note

No Notes found.

Platform information

Have you already reported the content? **Yes**

Social Media Username **s 47E(d), s 47F**

Respondent Username **--**

Date Reported **28/02/2024**

We will need to see evidence that you complained to the platform about cyberbullying material.

Content Still Online? **Yes**

Please provide the website URL where we can see the material

--

Do you have the complaint number or reference number from your complaint to the Platform? **No**

Receipt number or Complaint number

--

Please provide an explanation on why you have not reported the content

--

Assessment of material

s 47C, s 47E(d), s 47F

Complaint Categories

Name ↑	Source Type
Defamation	ACA
Hate speech	ACA
Nasty comments/name calling	ACA
Offensive/upsetting pictures or videos	ACA

Related Platform Usernames

s 47E(d), s 47F

1 - 4 of 5

Complained Locators

URL ↑	Type
https://twitter.com/BilboardChris/status/176262000169...	Complained
s 47E(d), s 47F	Complained
	Complained
	Complained

Related Capture Requests

Number	Capture Ty...	Progress	Complaint alert	Removal Notice	Serious cyberbullying	Serious cyber abuse	Created On ↓
No data available.							

System

Active

Legal Requests

Your request has been submitted and will be processed as soon as possible.

You will receive a confirmation email that includes a case number from support@twitter.com.
Please make sure to check your spam folder if you do not receive the confirmation.

More information for law enforcement is available in our [Guidelines for Law Enforcement](#). More information for civilians is available in our Help Center: [Requesting Twitter Data](#); [Requesting content removal](#).

Compliance and Enforcement Policy

eSC CEP

December 2021



Contents

Overview	3
Outline of eSafety’s compliance and enforcement powers	3
Considerations eSafety takes into account when determining compliance or enforcement action	6
Compliance options	9
Informal approaches	9
Removal notices	9
What is a removal notice?	9
When can a removal notice be issued?	10
Review rights	10
What are the consequences of a removal notice?	10
Scheme-specific information	11
Service provider notifications	11
What is a service provider notification?	11
What are the consequences of a service provider notification?	12
Enforcement powers	12
Formal warnings	12
What is a formal warning?	12
When can a formal warning be issued?	12
What are the consequences of not complying with a formal warning?	13
Enforceable undertakings	13
What is an enforceable undertaking?	13
When can an undertaking be accepted?	13
What does an enforceable undertaking contain?	13
What are the consequences of an enforceable undertaking?	14
Can an enforceable undertaking be varied or cancelled?	14
Injunctions	14
What is an injunction?	14
When can eSafety apply for an injunction?	15
What are the consequences of an injunction?	15
Can an injunction be discharged or varied?	15
Infringement notices	15
What is an infringement notice?	15
Who can give an infringement notice?	15

When can an infringement notice be given?	15
What does an infringement notice need to contain?	16
Amount payable under the infringement notices	16
What are the consequences of an infringement notice?	17
Can the recipient of an infringement notice seek to have it withdrawn?	17
Civil penalty orders	18
What is a civil penalty order?	18
Who can apply for a civil penalty order?	18
When can the Commissioner apply for a civil penalty order?	18
What are the consequences of a civil penalty order?	18
Can a civil penalty order be appealed?	18
Referral of matter to law enforcement	19
General investigative powers	20
Part 13 - information gathering powers	20
Penalties for failure to comply with the requirements of Part 13	20
Part 14 - compulsory examination and document production powers	21
Procedures	21
Penalties for failure to comply with the requirements of Part 14	22
Attachment A: Compliance and Enforcement Options Available to eSafety under the Act	23



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.

¹The 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 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.

²Online Safety Act 2021 (Cth), Part 4. ³Online 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 complaint?			
<p>An Australian child who has reason to believe they were or are the target of cyberbullying material (s 30(1) of the Act).</p> <p>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).</p> <p>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).</p>	<p>A person⁴ depicted in an intimate image who has reason to believe s 75 of the Act⁵ has been contravened (s 32(1)-(2) of the Act).</p> <p>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).</p>	<p>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).</p> <p>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).</p>	<p>A person who has reason to believe that Australians can access class 1 and certain class 2 material through an online service provider⁶ (s 38(1) of the Act).</p> <p>Or a person who has reason to believe that Australians can access certain class 2⁷ material through an online service provider and that access is not subject to a restricted access system (s 38(2) of the Act).</p>
Complaints process			
<p>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).</p>	<p>Complaints can be made about non-consensual posting (or threats of posting) of intimate images (s 32 of the Act).</p> <p>Objection notices can be given for intimate images including where the images were initially posted with consent (s 33 of the Act).</p>	<p>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).</p>	<p>Complaints can be made in relation to class 1 and class 2 material (s 38 of the Act).</p> <p>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).</p>

⁴Either the person depicted or the person who is posting or threatening to post the intimate image must be ordinarily resident in Australia. ⁵Section 75 of the Act prohibits posting or threatening to post an intimate image without the consent of the person shown in the images. ⁶Class 1 material is defined in s 106 of the Act and class 2 material is defined in s 107 of the Act. ⁷Material 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			
<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Service provider notifications (s 85 of the Act) • Removal notices (ss 77-79 of the Act) • Remedial directions (s 83 of the Act) 	<ul style="list-style-type: none"> • Service provider notifications (s 93 of the Act) • Removal notices (ss 88-90 of the Act) 	<ul style="list-style-type: none"> • 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 Act⁸ or under the concept of free speech generally
- any other factors that eSafety considers to be of relevance.

⁸Section 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-user⁹ (except in the Online Content Scheme¹⁰ and the Cyberbullying Scheme¹¹) 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 material¹³ notified by eSafety. A failure to do so is a breach of a civil penalty provision.¹⁴

⁹Online Safety Act 2021 (Cth), ss 70, 78 and 89. ¹⁰Under 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. ¹¹The 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). ¹²Online Safety Act 2021 (Cth), ss 65, 66, 77, 79, 88, 90, 109, 110, 114, 115. ¹³Except 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). ¹⁴Online 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.

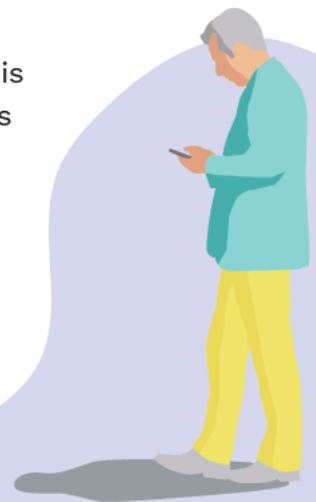
Review rights

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



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

¹⁹See 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.

²⁰Online Safety Act 2021 (Cth), ss 73(1), 85(1), 93(1). ²¹Online 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](#).

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

²⁴Online 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 Act²⁵ 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.

²⁵See [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 Act²⁶
- 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 conduct³⁴



²⁶Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(a). ²⁷Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(b).

²⁸Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(1)(c). ²⁹Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 115.

³⁰Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(3). ³¹Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 114(5).

³²The sections which can be subject to an injunction under the Act are set out in s 165(1) of the Act. ³³Online Safety Act 2021 (Cth), s 165(3). ³⁴Regulatory 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 action³⁵
- 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.

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

⁴³Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 103(2). ⁴⁴Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104.

⁴⁵Regulatory 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. ⁴⁶Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 104(3). ⁴⁷The 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



⁴⁸Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 107(1). ⁴⁹Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 105.

⁵⁰Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(1). ⁵¹Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(2).

⁵²Regulatory Powers (Standard Provisions) Act 2014 (Cth), s 106(3). ⁵³Regulatory 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

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

⁵⁸The 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 provider⁵⁹ 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](#).



⁵⁹A 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)). ⁶⁰Online Safety Act 2021 (Cth), s 194(1).

⁶¹Online 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 questions⁶² or to provide other information⁶³
- 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 investigation⁶⁴
- 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

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



⁷²Online Safety Act 2021 (Cth), s 205. ⁷³Online 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. ⁷⁴Online 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	✗	✗	✓	✓

⁷⁵Note 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). ⁷⁶SMS, 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	✗	✗	✗	✗



Adult Cyber Abuse Scheme Regulatory Guidance

eSC RG 3

Updated December 2023



Contents

Overview of this guidance	2
Overview of the Adult Cyber Abuse Scheme	2
Key terms	3
What is ‘adult cyber abuse’?	3
Who is meant by ‘a particular Australian adult’?	3
What is ‘serious harm’ in the context of the Adult Cyber Abuse Scheme?	4
How does eSafety determine ‘serious harm’ in the context of adult cyber abuse?	4
What is meant by ‘mere ordinary emotional reactions’?	4
What does ‘menacing, harassing or offensive’ mean?	5
Menacing or harassing	5
Offensive	5
Freedom of speech	6
Material that does not meet the threshold	6
Making a complaint to eSafety	6
Who can complain?	6
Complaint made by an Australian adult	7
Complaint made on behalf of an Australian adult	7
Making a complaint to online service providers first	7
Investigation of adult cyber abuse material	8
Approaches to compliance and enforcement	8
Informal requests	8
Formal actions	8
Compliance and enforcement options	9
Service provider notifications	10
What are service provider notifications?	10
When can eSafety issue a service provider notification under the Adult Cyber Abuse Scheme?	10
What are the consequences of a service provider notification?	10
Removal notices	11
What is a removal notice?	11
When can eSafety issue a removal notice under the Adult Cyber Abuse Scheme?	11
What are the consequences of a removal notice?	12
Taking enforcement action	12
Review rights	13
Basic Online Safety Expectations	13
Find more information and support	13

Overview of this guidance

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

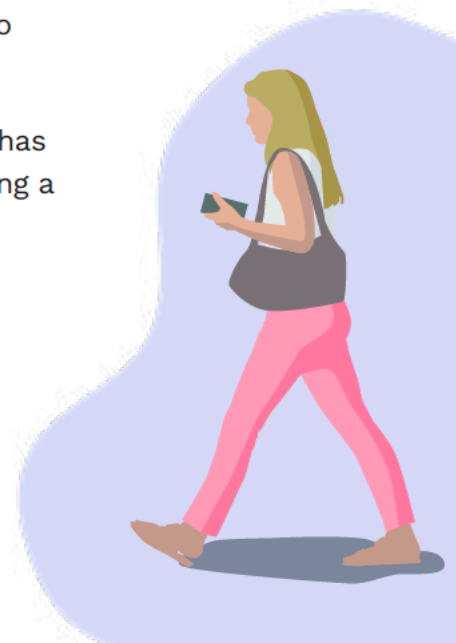
This information is for members of the general public, the online industry and other professionals who require further information about the Adult Cyber Abuse Scheme. It provides an overview of the actions available to eSafety under the Online Safety Act 2021 (the Act) to address adult cyber abuse. It 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 Act¹ 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.

¹Section 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.

²Section 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.

³Section 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, and⁴
- 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.



⁴Section 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.

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

⁹Sections 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.

¹⁰Section 37(1) of the Act. ¹¹Section 37(2) of the Act. ¹²Section 37(5) of the Act. ¹³Sections 197 to 205 of the Act. ¹⁴Sections 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		<p>Give one of the following service provider notifications:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>	<p>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.</p>
Take enforcement action	<p>Options for failing to comply with a removal notice:</p> <ul style="list-style-type: none"> • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. <p>Failure to comply with a Part 14 notice may also attract certain penalties.</p>	<p>Options for failing to comply with a removal notice:</p> <ul style="list-style-type: none"> • issuing a formal warning • accepting an enforceable undertaking • seeking a court injunction • issuing an infringement notice • seeking a civil penalty order. <p>Failure to comply with a Part 13 or Part 14 notice may also attract certain penalties.</p>

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.



¹⁵Section 93(1) of the Act. ¹⁶Section 93(1) of the Act. ¹⁷Section 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-user¹⁸ or to the provider of a social media service, relevant electronic service, designated internet service¹⁹ 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.

¹⁸Section 89 of the Act. ¹⁹Section 88 of the Act. ²⁰Section 90 of the Act. ²¹Section 88, 89 and 90 of the Act. ²²Section 90 of the Act. ²³Section 91 of the Act. ²⁴The 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)	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Generally, a person whose interests are affected by the notice
Refusing to give a removal notice (online service provider)	<ul style="list-style-type: none">• 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](https://www.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.

