

Complaint

CYR-0740083

Created On
2/01/2026 7:27 PM

Complaint Status
Under Investigation

Assigned To
s 22

Response Required
No

Summary

Date Received
2/01/2026 7:27 PM

Date Finalised

Complaint Status
Under Investigation

Assigned To
s 22

Source Type
CYR

Derived
No

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Police Involved
No

Education Provider
No

Complainant

Repeat Complainant
No

Complainant Reason
[Child sexual abuse / child abuse / Paedophile activity](#)

Response Required
No

Response Method

Submission

Method Received
Web Form

Presentation Type
Social media

Device Type
Mobile Phone

Device Name

Remote IP Address

Access Information

Additional access instructions
X's AI Grok is creating images sexualising children after users prompt it to

Access Username

Access Password

Related Entities

URL	Type	Type	S...	Investigation Id	Status	Investigated Loc
s 47E(d)	Complained	Social Media Se	■	INV-2026-00127	Not Actionable	s 47E(d)
	Complained	Social Media Se	■	INV-2026-00126	Not Actionable	
	Complained	Social Media Se	■	INV-2026-00125	Not Actionable	
	Complained	Social Media Se	■	INV-2026-00124	Assessment in Progress	

1 - 4 of 4 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
0 - 0 of 0 (0 selected)			

Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
s 47E(d)

Grok

1 - 1 of 1 (0 selected)

Page 1

Complaint

CYR-0741593

Created On
5/01/2026 11:12 AM

Complaint Status
New

Assigned To
s 22

Response Required
Yes

Summary

Date Received
5/01/2026 11:12 AM

Complaint Status
New

Source Type
CYR

Complainant

Anonymous Complaint
No

Australian Resident
Yes

Complainant

s 47F

Complainant Reason
Child sexual abuse / child abuse /
Paedophile activity

Date Finalised

Assigned To
s 22

Derived
No

Police Involved
No

Repeat Complainant
No

Response Required
Yes

Education Provider
No

Response Method
E-mail

Title: CYR-0741593 Assessment

No access details were provided, eSafety Enquiries team are coordinating responses. Referral sent on 14-Jan-26

s 22 14/01/2026 9:56 AM

Submission

Method Received
Web Form

Device Type
Mobile Phone

Remote IP Address

Presentation Type
Social media

Device Name

Access Information

Additional access instructions

The app X (formerly twitter) has a built in AI chat bot, which currently allows you to put in images of anyone (minor or adult) and tell it to remove their clothing in which it does. s 47F

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
	Complained	Social Media Se		

1 - 1 of 1 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
0 - 0 of 0 (0 selected) Page 1			

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status
14/01/2026 10:34 AM	eSafety Enquiries	Cyber Report; Cyber Report; Cyber ...	RE: IRCT referral for Enquiries response – Grok AI CYR-07...	Received
14/01/2026 9:55 AM	Cyber Report	eSafety Enquiries	IRCT referral for Enquiries response – Grok AI CYR-07415...	Sent

1 - 2 of 2 (0 selected) Page 1

Assessment

Content Tags

Name

Grok

..... 1 - 1 of 1 (0 selected)

Page 1

Investigation

INV-2026-00127

Created
5/01/2026 12:18 PM

Investigation Status
Not Actionable

Investigator
s 22

Outcome

Summary

s 47E(d)

Content Service Type
Social Media Service (SMS)

Complainant Reason
[Child sexual abuse / child abuse / Paedophile activity](#)

Priority
Low

Investigator
s 22

Created
5/01/2026 12:18 PM

Derived
No

Referrer Url

Presentation Type
Social media

Type
OSA Section 38

Technical Element
No

Investigation Status
Not Actionable

Commenced
5/01/2026

Finalised

Source Type
CYR

Title:
INV re-opened due to a capture folder and trace details being unavailable. Material has not changed.

s 22 14/01/2026 10:11 AM

Title:
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.

s 22 8/01/2026 2:55 PM

Content

Locator Documents

Investigation Documents

Content Traces

Source IP	Primary Record	Hosting Country	Date
162.159.140.229	Yes	United States	14/01/2026 10:11 AM
1 - 1 of 1 (0 selected)			Page 1

Regulatory Notices

Name	Notice Type	Legislative Reference	Date Sent	Due Date	Outcor
No Regulatory Notice records are available in this view.					
0 - 0 of 0 (0 selected)					Page 1

INHOPE

Reference Number

Referral Sent

Report Status

Actions

Report to LEA
No

Report to ISP
No

Content Removed
No

Content Unavailable
No

Moved
No

Not Illegal
No

Not Legally Accessible
No

Status Update

Last status update

Next status update

Related Emails

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				
0 - 0 of 0 (0 selected)				Page 1

Status **Not Actionable**

Investigation

INV-2026-00126

Created
5/01/2026 12:18 PM

Investigation Status
Not Actionable

Investigator
s 22

Outcome

Summary

Locator
s 47E(d)

Content Service Type
Social Media Service (SMS)

Complainant Reason
[Child sexual abuse / child abuse / Paedophile activity](#)

Priority
Low

Investigator
s 22

Created
5/01/2026 12:18 PM

Derived
No

Referrer Url

Presentation Type
Social media

Type
OSA Section 38

Technical Element
Yes

Investigation Status
Not Actionable

Commenced
5/01/2026

Finalised
14/01/2026

Source Type
CYR

Title:
INV re-opened due to a capture folder and trace details being unavailable. Material has not changed.

s 22 14/01/2026 10:11 AM

Title:
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.

s 22 8/01/2026 2:56 PM

Title: CDR

s 22 5/01/2026 2:23 PM

Content

Locator Documents

Investigation Documents

Content Traces

Source IP	Primary Record	Hosting Country	Date
162.159.140.229	Yes	United States	14/01/2026 10:10 AM
1 - 1 of 1 (0 selected)			Page 1

Regulatory Notices

Name	Notice Type	Legislative Reference	Date Sent	Due Date	Outcor
No Regulatory Notice records are available in this view.					
0 - 0 of 0 (0 selected)					Page 1

INHOPE

Reference Number

Referral Sent

Report Status

Actions

Report to LEA
No

Report to ISP
No

Content Removed
No

Content Unavailable
No

Moved

No

Not Illegal

No

Not Legally Accessible

No

Status Update

Last status update

Next status update

Related Emails

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				
0 - 0 of 0 (0 selected)				Page 1

Status **Not Actionable**

Investigation

INV-2026-00125

Created
5/01/2026 12:18 PM

Investigation Status
Not Actionable

Investigator
s 22

Outcome

Summary

Locator
s 47E(d)

Content Service Type
Social Media Service (SMS)

Complainant Reason
Child sexual abuse / child abuse / Paedophile activity

Priority
Low

Investigator
s 22

Created
5/01/2026 12:18 PM

Derived
No

Referrer Url

Presentation Type
Social media

Type
OSA Section 38

Technical Element
Yes

Investigation Status
Not Actionable

Commenced
5/01/2026

Finalised

Source Type
CYR

Title:
INV re-opened due to a capture folder and trace details being unavailable. Material has not changed.
s 22 14/01/2026 10:12 AM

Content

Locator Documents

Investigation Documents

Content Traces

Source IP	Primary Record	Hosting Country	Date	Time
162.159.140.229	Yes	United States	14/01/2026	10:09 AM
1 - 1 of 1 (0 selected)			Page 1	

Regulatory Notices

Name	Notice Type	Legislative Reference	Date Sent	Due Date	Outcor
No Regulatory Notice records are available in this view.					
0 - 0 of 0 (0 selected)					Page 1

INHOPE

Reference Number

Referral Sent

Report Status

Actions

Report to LEA
No

Report to ISP
No

Content Removed
No

Content Unavailable
No

Moved

No

Not Illegal

No

Not Legally Accessible

No

Status Update

Last status update

Next status update

Related Emails

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				
0 - 0 of 0 (0 selected)				Page 1

Status **Not Actionable**

Investigation

INV-2026-00124

Created
5/01/2026 12:18 PM

Investigation Status
Not Actionable

Investigator
s 22

Outcome

Summary

Locator
s 47E(d)

Content Service Type
Social Media Service (SMS)

Complainant Reason
Child sexual abuse / child abuse / Paedophile activity

Priority
Low

Investigator
s 22

Created
5/01/2026 12:18 PM

Derived
No

Referrer Url

Presentation Type
Social media

Type
OSA Section 38

Technical Element
Yes

Investigation Status
Not Actionable

Commenced
5/01/2026

Finalised
16/01/2026

Source Type
CYR

Title:
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.

s 22 16/01/2026 2:36 PM

Content

Locator Documents

Investigation Documents

Content Traces

Source IP	Primary Record	Hosting Country	Date
172.66.0.227	Yes	United States	14/01/2026 9:44 AM
1 - 1 of 1 (0 selected)			Page 1

Regulatory Notices

Name	Notice Type	Legislative Reference	Date Sent	Due Date	Outcor
No Regulatory Notice records are available in this view.					
0 - 0 of 0 (0 selected)					Page 1

INHOPE

Reference Number

Referral Sent

Report Status

Actions

Report to LEA
No

Report to ISP
No

Content Removed
No

Content Unavailable
No

Moved

No

Not Illegal

No

Not Legally Accessible

No

Status Update

Last status update

Next status update

Related Emails

Date Sent/Received	From	To	Subject	Status
No E-mail records are available in this view.				
0 - 0 of 0 (0 selected)				Page 1

Status

Not Actionable

Complaint

CYR-0742725

Created On
7/01/2026 4:26 PM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary

Date Received
7/01/2026 4:26 PM

Complaint Status
Not Actionable

Source Type
CYR

Complainant

Anonymous Complaint Yes
Australian Resident Yes

Complainant

Complainant Reason
 Extreme, offensive or adult content

Submission

Method Received
Web Form

Device Type
Mobile Phone

Remote IP Address

Access Information

Additional access instructions

X users can use the Grok AI service to create "deepfake" style images of other users' images, ie altering/reducing clothing including creating sexualised images of minors. This has been reported by many media outlets and I have attached some examples here. This may be in violation of relevant Australian law.

Date Finalised

Assigned To
s 22

Derived
No

Police Involved No
Education Provider No

Repeat Complainant
No

Response Required No
Response Method

Presentation Type
Social media

Device Name

Title: NA –

NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.


s 47E(d)

s 22 9/01/2026 9:57 AM

Title: NA –

NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.

s 47E(d)

 2026-01-09_09-30-04.png

s 22 9/01/2026 9:31 AM

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loca
s 47E(d)	Complained	Social Media Se		
	Complained	Social Media Se		
	Complained	Social Media S		

0 - 0 of 0 (0 selected) Page 1

1 - 3 of 3 (0 selected) Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
Grok

Nonactionable (Unrestricted/MA15+ and below)

1 - 2 of 2 (0 selected)

Page 1

Complaint

CYR-0742940

Created On
8/01/2026 11:16 AM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary

Date Received
8/01/2026 11:16 AM

Complaint Status
Not Actionable

Source Type
CYR

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Complainant

Complainant Reason
[Child sexual abuse / child abuse / Paedophile activity](#)

Submission

Method Received
Web Form

Device Type
Mobile Phone

Remote IP Address

Access Information

Additional access instructions

Due to the new image generation capabilities added to X's AI Grok, users are now altering images of children and women to show them in bikinis and without clothes. This is abhorrent and illegal, and due to the X algorithm pushing content users do not follow, the risk of seeing it cannot be avoided if one uses X at all. This has been widely reported in media and something must be done.

Date Finalised

Assigned To
s 22

Derived
No

Police Involved
No

Education Provider
No

Repeat Complainant
No

Response Required
No

Response Method

Presentation Type
Social media

Device Name

Title:

NA – No Content. There is no material to action. No content was available at the time of assessment. The material has been removed or is unavailable.

s 22 8/01/2026 2:21 PM

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
	Complained	Social Media Se		

1 - 1 of 1 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
	INV-2024-04213	Invalid Complaint	(No name)

0 - 0 of 0 (0 selected) Page 1

1 - 1 of 1 (0 selected) Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
AI (Artificial Intelligence)

Grok

1 - 2 of 2 (0 selected)

Page 1

From: Codes
Sent: Thursday, 8 January 2026 5:02 PM
To: 47F [REDACTED]@x.com
Cc: 47F [REDACTED] s 22 [REDACTED]; s 22 [REDACTED]; Codes
Subject: Correspondence from eSafety's General Manager - CSEM on X [SEC=OFFICIAL]
Attachments: 20260108 Letter to X re CSEM and Grok.pdf

OFFICIAL

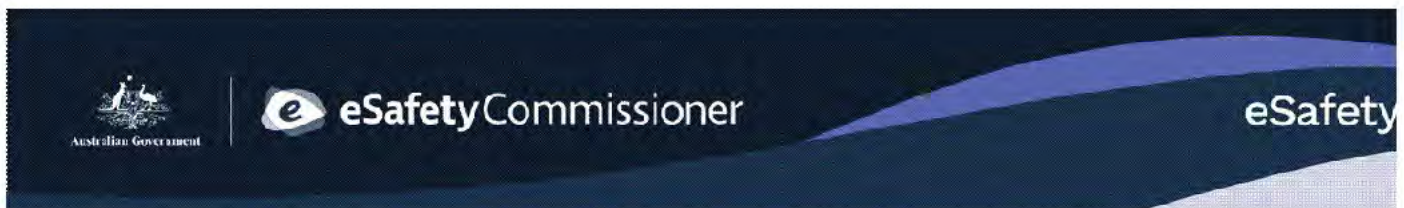
Dear s 47F [REDACTED],

Please find attached correspondence from eSafety's General Manager of Regulatory Operations in relation to child sexual exploitation material on X.

The correspondence requests your response by 16 January 2026.

Kind regards,

eSafety



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.

8 January 2026

s 47F

X

By email: s 47F @x.com

Dear s 47F,

Further to eSafety's correspondence of 13 May 2025, 17 April 2025, 8 April 2025, 15 October 2024 and 27 August 2024, we remain concerned that eSafety continues to identify child sexual exploitation material (**CSEM**) widely advertised and shared on X, including in a manner likely to expose the public to this extremely harmful material.

Despite the comments made by X's Chief Executive Officer over three years ago that 'removing child exploitation is priority #1'¹ and your statement recently on a call with eSafety on 26 November 2025 that child safety was a priority for X, the availability of CSEM continues to appear particularly systemic on X. eSafety has not identified CSEM to be as readily accessible on any other mainstream service.

While X's actions to address bot accounts in October 2025 appears to have had an impact on the use of some previously commonly used hashtags and terms to advertise CSEM, the measures appear to have been inadequate and ineffective at preventing continued widespread dissemination of CSEM and use of hashtags to advertise this material.

We are concerned that apparently innocuous hashtags appear to be coopted to advertise CSEM, particularly when used together. eSafety found CSEM amongst other material using combinations of the hashtags: s 7(2) The fact that some of these terms have innocuous uses means users are likely to be inadvertently exposed to CSEM despite seeking to use the X service in a legitimate manner.

While X takes action on eSafety's content notifications for specific CSEM, X's responsibilities are broader than such reactive action. As you are aware, regardless of whether X is regulated

¹ Elon Musk, X; 24 November 2022, URL

https://x.com/elonmusk/status/1595671290421170179?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Cwterm%5E1595671290421170179%7Ctwgr%5E53a53c8fc533c1315c5e66f1d91fa41200f99497%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2022-11-29%2Fmusk-s-cuts-decimated-twitter-team-tackling-child-sexual-abuse

under the *Social Media Services Online Safety Code (Class 1A and Class 1B Material)* or the *Online Safety (Relevant Electronic Services— Class 1A and Class 1B Material) Industry Standard 2024*, it is required to proactively detect, disrupt and deter CSEM.

Our concerns regarding CSEM on X have been accentuated by recent reporting regarding the Grok AI-feature on X generating ‘undressing’ images of children and adults, in breach of X and Grok’s own terms of service. Even more concerning, the Internet Watch Foundation has reported that material generated includes depictions of child sexual abuse of children between 11 and 13.² eSafety is currently reviewing a number of complaints about ‘undressing’ material generated by Grok on X and, subject to that assessment, will consider whether to issue removal notices to X under the *Online Safety Act 2021* (Cth) (the **Act**), and/or take other actions.

X’s statement³ on 4 January 2026 regarding this activity referred to removing relevant material and suspending accounts involved, but did not refer to any changes X intended to implement on its service to prevent future misuse of Grok on X from taking place.

In addition to the ‘undressing’ material, recent analysis by AI Forensics suggests Grok is also generating terrorist content and posting it on X.⁴

In relation to the industry codes and standards under the Act, while Grok is also a separate service and regulated under the *Online Safety (Designated Internet Services— Class 1A and Class 1B Material) Industry Standard 2024*, X is responsible for the feature’s implementation on the X service.

We request you respond to this correspondence by 16 January 2026 with any actions X has taken, or will take, in relation to:

1. the ongoing prevalence of CSEM on X including the use of common hashtags to advertise this material;

² Sky News, quotes from Ngaire Alexander, head of hotline at the Internet Watch Foundation, 7 January 2026, URL: <https://news.sky.com/story/illegal-child-abuse-material-generated-by-xs-artificial-intelligence-grok-says-uk-watchdog-13491658>

³ X Safety; 4/1/2026: URL https://x.com/safety/status/2007648212421587223?s=46&t=sfB_goPNqOx9v0Ysp-oHIA

⁴ AI Forensics Post and Report on LinkedIn, 7 January 2026, URL: https://www.linkedin.com/posts/aiforensics_grok-ai-images-activity-7414252008783646720-j7AO?utm_source=li_share&utm_content=feedcontent&utm_medium=g_dt_web&utm_campaign=copy

2. the generation by Grok on X of 'undressing' material involving adults and children; and
3. minimising, disrupting and deterring the generation by Grok of CSEM and pro-terror material on X.

This request is voluntary. However, any information you choose to provide will be used to assess X's compliance with its relevant obligations.

eSafety will not regard any response from X as privileged.

Yours sincerely,

s 22



General Manager, Regulatory Operations

Complaint

CYR-0743126

Created On
8/01/2026 8:55 PM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary

Date Received
8/01/2026 8:55 PM

Complaint Status
Not Actionable

Source Type
CYR


Date Finalised
9/01/2026

Assigned To
s 22

Derived
No

Title:
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (adult content) material under sections 106 and 107 of the OSA.

s 22 9/01/2026 10:02 AM

Title:
 Screenshot_9-1-2026_10143_x.com.jpeg

s 22 9/01/2026 10:02 AM

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Police Involved
No

Education Provider
No

Complainant

Repeat Complainant
No

Complainant Reason
 [Child sexual abuse / child abuse / Paedophile activity](#)

Response Required
No

Response Method

Submission

Method Received
Web Form

Presentation Type
Web Page

Device Type
PC/Laptop

Device Name

Remote IP Address

Access Information

Additional access instructions
Grok for weeks has been allowing deepfakes of any photo of the site, which includes children. Reports are rife or CSAM, torture, sexual abuse etc. WHY IS X STILL AVAILABLE IN AUSTRALIA?

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
s 47E(d)	Complained	Designated Inter		

1 - 1 of 1 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
█	INV-2025-09886	Not Actionable	https://x.com/

1 - 1 of 1 (0 selected) Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
Grok

1 - 1 of 1 (0 selected) Page 1

From: s 47F [redacted]@x.com>
Sent: Thursday, 8 January 2026 5:46 PM
To: Codes
Cc: s 47F [redacted]; s 22 [redacted]; s 22 [redacted]; s 47F [redacted]
Subject: Re: Correspondence from eSafety's General Manager - CSEM on X [SEC=OFFICIAL]

Dear eSafety

Thank you for your email and letter - I acknowledge receipt and we will revert.

Kind regards

s 47F [redacted]

On Thu, 8 Jan 2026 at 06:01, Codes s 47E(d) [redacted]@esafety.gov.au> wrote:

OFFICIAL

Dear s 47F [redacted]

Please find attached correspondence from eSafety's General Manager of Regulatory Operations in relation to child sexual exploitation material on X.

The correspondence requests your response by 16 January 2026.

Kind regards,

eSafety



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.

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.

From: s 47F @ofcom.org.uk>
Sent: Saturday, 10 January 2026 3:39 AM
To: s 22 ; Julie Inman Grant
Cc: s 22 ; s 22 ; s 47F ; s 47F ; s 22 ;
s 22
Subject: RE: EXTERNAL:RE: Concerns about NCII or CSAM on X and Grok [SEC=OFFICIAL]

s 22 , thanks so much for the rapid response on this – it's much appreciated. Very happy to compare notes once we've decided our next move – we're expecting to say more about that next week. And we may well come back to you with more detailed questions further down the line. For now, very many thanks again.

s 47F

From: s 22 @eSafety.gov.au>
Sent: 09 January 2026 05:39
To: Julie Inman Grant s 47E(d) @eSafety.gov.au>; s 47F @ofcom.org.uk>
Cc: s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22 @ofcom.org.uk>; s 47F @ofcom.org.uk>; s 22 @esafety.gov.au>; s 22 @esafety.gov.au>; s 22 @esafety.gov.au>; s 22 @esafety.gov.au>
Subject: EXTERNAL:RE: Concerns about NCII or CSAM on X and Grok [SEC=OFFICIAL]

CAUTION: This email originated outside your organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

OFFICIAL

Hi s 47F ,

Thanks for getting in touch. Some relevant internal information regarding the Grok 'undressing' material is set out below, as well as the broader availability of child sexual exploitation material (CSEM) on X. We also published a media statement today [eSafety raises concerns about misuse of Grok to generate sexualised content | eSafety Commissioner](#)

Please treat the below in confidence and consult eSafety before any disclosure.

Grok

- eSafety has received 14 reports via our complaints schemes in relation to 'undressing' material produced Grok on X since late 2025, as well as a range of broader correspondence raising concerns. We are assessing reported material to ascertain whether any is CSEM or image based abuse of adults as defined in the Online Safety Act.
 - We consider at least one report constitutes image based abuse and is still available on X. We are considering appropriate actions, which may include notifying X and/or issuing

removal notices. Another complaint also met the threshold but the material has since been removed.

s 37(1)(a)

X and CSEM

- We have long been concerned about how readily identifiable CSEM is on X, often advertised using common hashtags. We do not find CSEM to be so easily accessed on other mainstream social media services. CSEM identified by eSafety on X includes high end material, including contact abuse of pre-pubescent children. We have shared these concerns with X on multiple occasions over the last 18 months in correspondence and meetings.
- X responds to eSafety's notifications and removal notices regarding CSEM by removing the material. However our concern is whether they are appropriately detecting, disrupting and deterring this material and taking steps to minimise future distribution, which are relevant requirements under the applicable industry standard under the Act.
- As a result of these concerns, we commenced an investigation into X's compliance with the applicable industry standard in October 2025.
 - X is judicially reviewing the application of the relevant industry standard to their service, arguing a different industry code should apply. These proceedings are ongoing.
- eSafety has current civil penalty proceedings against X for alleged non-compliance with a transparency notice focussed on CSEM. X are actively defending the proceedings, including by challenging the validity of eSafety's notice on the basis that it does not comply with the requirements of the Online Safety Act. Our civil penalty proceedings follow on from X's judicial review of the transparency notice, which was dismissed on first instance and on appeal.

As Julie mentions, we wrote to X regarding our concerns regarding CSEM and Grok this week in the context of their obligations under the industry codes and standards.

Let us know if it would be helpful to arrange a call next week or any other time to discuss further.

Best,

s 22

Enforcement Taskforce

s 22

From: Julie Inman Grant s 47E(d) <Julie.Inman.Grant@eSafety.gov.au>

Sent: Friday, 9 January 2026 7:00 AM

To: s 47F <s47f@ofcom.org.uk>; s 22 <s22@esafety.gov.au>; s 22

s 22 <s22@esafety.gov.au>

Cc: s 22 <s22@eSafety.gov.au>; s 22 <s22@eSafety.gov.au>; s 22

<s47f@esafety.gov.au>; s 47F <s47f@ofcom.org.uk>; s 47F

<s47f@ofcom.org.uk>

Subject: Re: Concerns about NCII or CSAM on X and Grok

Thanks s 47F. We are indeed concerned and reached out to X Corp yesterday with some specific questions building on some investigative work around CSAM on the platform we have been doing for some time. s 22 and s 22 are taking the lead on this one but I do think it would be good to compare notes here and see how we might leverage our respective approaches. Thank you for reaching out!

Julie

Get [Outlook for iOS](#)

From: s 47F @ofcom.org.uk>
Sent: Friday, January 9, 2026 5:18:08 AM
To: Julie Inman Grant s 47E(d) @eSafety.gov.au>; s 22 @esafety.gov.au>
Cc: s 22 @eSafety.gov.au>; s 22 @eSafety.gov.au>; s 22 esafety.gov.au>; s 47F @ofcom.org.uk>; s 47F @ofcom.org.uk>
Subject: Concerns about NCII or CSAM on X and Grok

Classification: CONFIDENTIAL

Dear Julie, s 22

I hope you're both well. I'm afraid 2026 has not started the way any of us would have wanted from an online safety perspective. I expect you'll have seen that we've urgently contacted X and X.AI about the allegations that Grok has been used to generate non-consensual intimate images of adults, as well as potentially sexualised images of children that could constitute CSAM.

I saw Julie's comments on LinkedIn yesterday about the reports you've received. Is there any further information you can share at this time? Specifically any further high-level insight you can share on:

- the presence of NCII or CSAM on X that may have been generated by Grok.
- X.AI's processes for - or challenges in - preventing such content from being generated.
- whether X is swiftly removing such content once reported.

We have a very tight timetable I'm afraid! We're due to decide our next steps on Monday, so this is a request for any high-level insight you might have, **in your current working day**, that you can easily share. If that's not possible, that's no problem – we may follow up with a more formal request in due course, as our work progresses, but would be very interested in what you can share now. Many apologies for the quick turnaround.

Lastly on a personal note I know you've experienced this horrible abuse personally before, as have a number of our female colleagues. You have our greatest sympathy. Of course if there is anything we can do to support your work in this area please let us know.

Best wishes

s 47F

I'm sending this at a time that fits my working pattern and family commitments – please read/respond when it's convenient for you.

s 47F

:: Ofcom

Riverside House
2a Southwark Bridge Road
London SE1 9HA
www.ofcom.org.uk

For more information visit www.ofcom.org.uk

This email (and any attachments) is confidential and intended for the use of the addressee only.

If you have received this email in error please notify the originator of the message and delete it from your system.

This email has been scanned for viruses. However, you open any attachments at your own risk.

Any views expressed in this message are those of the individual sender and do not represent the views or opinions of Ofcom unless expressly stated otherwise.

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.

For more information visit www.ofcom.org.uk

This email (and any attachments) is confidential and intended for the use of the addressee only.

If you have received this email in error please notify the originator of the message and delete it from your system.

This email has been scanned for viruses. However, you open any attachments at your own risk.

Any views expressed in this message are those of the individual sender and do not represent the views or opinions of Ofcom unless expressly stated otherwise.

Complaint

CYR-0744174

Created On
10/01/2026 9:36 PM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary


Date Received
10/01/2026 9:36 PM

Date Finalised

Title: NA –
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA.

Complaint Status
Not Actionable

Assigned To
s 22

 2026-01-13_14-17-10.png
s 22 13/01/2026 2:17 PM

Source Type
CYR

Derived
No

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Police Involved
No

Education Provider
No

Complainant

Repeat Complainant
No

Complainant Reason
 [Child sexual abuse / child abuse / Paedophile activity](#)

Response Required
No

Response Method

Submission

Method Received
Web Form

Presentation Type
Mobile Application

Device Type
Mobile Phone

Device Name

Remote IP Address

Access Information

Additional access instructions
Grok App is able to produce child exploitation material in its imagine image creator. This needs to be stopped immediately or the app access stopped.

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
Complained Designated Inter				
1 - 1 of 1 (0 selected)				Page 1

S...	Investigation Id	Status	Investigated Loca
0 - 0 of 0 (0 selected)			
0 - 0 of 0 (0 selected)			Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		
0 - 0 of 0 (0 selected)		Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				
0 - 0 of 0 (0 selected)				Page 1

Assessment

Content Tags

Name	
Grok	
1 - 1 of 1 (0 selected)	Page 1

Complaint

CYR-0744210

Created On
11/01/2026 12:41 AM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary

Date Received
11/01/2026 12:41 AM

Complaint Status
Not Actionable

Source Type
CYR

Date Finalised

Assigned To
s 22

Derived
No

Title: NA –

NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (restricted content) material under sections 106 and 107 of the OSA s 47E(d)

2026-01-13_14-24-37.zip
s 22 13/01/2026 2:26 PM

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Police Involved
No

Education Provider
No

Complainant

Repeat Complainant
No

Complainant Reason
[Child sexual abuse / child abuse / Paedophile activity](#)

Response Required
No

Response Method

Submission

Method Received
Web Form

Presentation Type
Social media

Device Type
PC/Laptop

Device Name

Remote IP Address

Access Information

Additional access instructions

Child pornography is being generated on Twitter using grok. People are asking the AI to put children in micro-bikinis. I feel this constitutes child pornography.

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
s 47E(d)	Complained	Social Media Se		
	Complained	Social Media Se		

0 - 0 of 0 (0 selected) Page 1

1 - 2 of 2 (0 selected) Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
AI (Artificial Intelligence)
Grok

1 - 2 of 2 (0 selected) Page 1



Complaint

CYR-0744742

Created On
11/01/2026 3:30 PM

Complaint Status
New

Assigned To
s 22

Response Required
No

Summary

Date Received
11/01/2026 3:30 PM

Date Finalised

Complaint Status
New

Assigned To
s 22

Source Type
CYR

Derived
No

Complainant

Anonymous Complaint
Yes

Australian Resident
Yes

Police Involved
No

Education Provider
No

Complainant

Repeat Complainant
No

Complainant Reason
[Sexually explicit](#)

Response Required
No

Response Method

Submission

Method Received
Web Form

Presentation Type
Social media

Device Type
Mobile Phone

Device Name

Remote IP Address

Access Information

Additional access instructions

X is continuing to allow registered users to create explicit pornographic fake imaging thru its Grok AI app. This action is a direct violation of its legal obligations and it should be shut down immediately


Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
	Complained	Social Media Se		

1 - 1 of 1 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
	INV-2024-11466	Terminated	(No name)

0 - 0 of 0 (0 selected) Page 1

1 - 1 of 1 (0 selected) Page 1

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
Grok

1 - 1 of 1 (0 selected) Page 1

From: s 47E(d) @esafety.gov.au
Sent: Monday, 12 January 2026 11:56 AM
To: s 47F ; s 47E(d) @esafety.gov.au
Subject: RE: eSafety Contact Us Submission #ENQ-0024333 CRM:0244000002861
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety Enquiries

The eSafety Commissioner

Enquiry ID	ENQ-0024333
Enquiry Type	Image Based Abuse
Due Date	16-Jan-2026 08:00 AM
Organisation	
Name	s 47F [REDACTED]
Email	s 47F [REDACTED]
Phone	
Subject	X and CSAM
Details	Why is there not a warning on the very front page about the reams of CSAM and other abuse materials being created via Grok on the x.com website?
Response Method	Email
Submitted Date	08-Jan-2026 20:57 PM
Hermes ID	6bc22f09-6850-4458-87ad-d2f1052beaed

From: s 47E(d) @esafety.gov.au
Sent: Monday, 12 January 2026 11:58 AM
To: s 47F ; s 47E(d) @esafety.gov.au
Subject: RE: eSafety Contact Us Submission #ENQ-0024261 CRM:0244000002828
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety Enquiries

The eSafety Commissioner



Australian Government



eSafety Commissioner

Enquiry ID	ENQ-0024261
Enquiry Type	Image Based Abuse
Due Date	13-Jan-2026 16:40 PM
Organisation	
Name	s 47F
Email	s 47F
Phone	
Subject	Deepfaking AI on "X.com"
Details	<p>All your reporting tools seem to be about individual acts, when the problem is that X.COMs AI GROK is currently publishing thousands upon thousands of deepfaked nude and sexual images including of children. Obviously many, many Australians are included in this.</p> <p>I don't understand how this isn't a primary concern of the commissioner or on our news - it's a huge site and this is a huge thing happening right on the front page.</p> <p>Is publishing deepfaked sexual imagery and forced nudity, especially of children, not the serious crime i've always assumed it to be?!</p>
Response Method	Email
Submitted Date	06-Jan-2026 16:36 PM
Hermes ID	26627b8f-caec-4b82-80e2-baf8629f108a

From: s 47E(d) @esafety.gov.au
Sent: Monday, 12 January 2026 2:11 PM
To: s 47F
Subject: RE: eSafety Contact Us Submission #ENQ-0022056 CRM:0244000001144
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hello s 47F,

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,
eSafety enquiries
The 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.

From: s 47F
Sent: Saturday, 10 January 2026 9:48 AM
To: s 47E(d) @esafety.gov.au
Subject: RE: eSafety Contact Us Submission #ENQ-0022056 CRM:0244000001144 [SEC=OFFICIAL:Sensitive]

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

Hello, happy 2026.

I was hoping to get a response to my response below, but now I have to add about Grok generating actual CSAM and it *not* immediately being banned. I know this has been through many social media channels, but what is the official eSafety response to X/Grok still generating CSAM and it being available in Australia?

I've also read the reports that image generation is now only for paid users is also false... because the source is Grok itself; and people are still generating it.

Regards,
s 47F

On Monday, 8 December 2025 at 07:16, s 47F wrote:

Hello,

I appreciate the time taken to reply, however the contents of the reply do not address any of the concerns I raised. The reply is a collection of motherhood statements from existing communications, and are proven by my cited research to be ineffective at best and damaging at worst.

There have been numerous high profile breaches as a result of existing age verification law requirements, resulting in the images and personal details of minors and adults being available on the dark web. How do you propose your social media laws will prevent this?

There has been numerous research historical and month-recent that shows that the age verification laws are damaging to children and do not protect children. I have quoted them below. How do you propose your social media laws are different?

all of the responsible research points to at-device protections that devices have had for a long time. The department of education has network controls at their disposal on managed devices that can be used. Why are we adopting the internationally disproven model of social media bans, where education and government support are the only way children actually get protected?

I really encourage decision makers to read the research and the current real world effects the US and EU laws have, the latest I can find on the real world results is a 404 media article - <https://www.404media.co/missouri-age-verification-law-porn-id-check-vpns/>

Regards,
s 47F

On Monday, 1 December 2025 at 16:04, s 47E(d) @esafety.gov.au <s 47E(d) @esafety.gov.au> wrote:

OFFICIAL: Sensitive

Dear s 47F,

Thank you for your email regarding the social media minimum age.

The new laws on the social media minimum age obligation require age-restricted social media platforms to take reasonable steps to prevent children under 16 from having an account on their platform. The obligation will take effect on 10 December 2025. The legislation was introduced and passed by the Parliament in 2024. eSafety does not have the power to change these laws. As the independent regulator for online safety in Australia, our role is to implement and enforce these laws.

We have shared our preliminary view on which platforms will be age-restricted here: [which platforms are age-restricted? | eSafety Commissioner](#). For more information on the social media minimum age, you can see our [frequently asked questions](#).

Privacy and safety are not mutually exclusive objectives and age assurance measures can be implemented in ways that protect user privacy. The [Office of the Information Commissioner](#) (OAIC) has an important role in monitoring and enforcing compliance with the privacy provisions set out in the Social Media Minimum Age legislation and under the Privacy Act, and eSafety is working closely with the OAIC to ensure that services preserve and protect user privacy when complying with the Social Media Minimum Age legislation. For more information about privacy and the social media minimum age, you might like to look at the [guidance for industry](#) the OAIC recently published.

We want to make sure that we are supporting young people and their community through these changes. We encourage you to visit our [social media age restrictions hub](#) which includes dedicated resources for [parents and carers](#) as well as specific resources for [young people](#) to help them understand and prepare for these changes.

eSafety will continue to take a holistic approach to protecting, supporting and empowering all Australians online, and will continue to work with communities, educators, parents, carers and young people through our Youth Council, to

promote online safety for all Australians. For more information about what we do, you can visit esafety.gov.au.

If you have further questions related to data and privacy matters, or you are concerned that you have been impacted by a data breach, we encourage you to visit the [Office of the Information Commissioner](https://www.oaic.gov.au) website.

Regards,

eSafety Enquiries

The eSafety Commissioner



Enquiry ID	ENQ-0022056
Enquiry Type	Other
Due Date	23-Oct-2025 08:00 AM
Organisation	
Name	s 47F
Email	s 47F
Phone	
Subject	Child protection doesnt
Details	Hi Putting up the top the latest issue with age verification laws - https://www.404media.co/the-discord-hack-is-every-users-worst-nightmare/ Social media bans don't protect kids. You've got access

to all the research that proves this. Some of the ones I have

<https://pubmed.ncbi.nlm.nih.gov/39809912/> Australia's social-media ban won't work - there are better ways to keep kids safe

<https://www.bandt.com.au/social-media-hurts-teens-but-banning-it-may-too-reveals-nature-study/> A review of the above if you don't have access to Nature.com

<https://humanities.org.au/uncategorised/an-age-ban-on-social-media-is-unworkable-what-are-the-alternatives/> An age ban on social media is unworkable - what are the alternatives?

<https://www.abc.net.au/news/2025-01-07/social-media-ban-mental-health-different-approach/104789108>

Queensland researchers say evidence linking social media to youth mental health problems is 'weak'

* <https://www.freezenet.ca/another-analysis-concludes-that-age-verification-doesnt-work/>

Beyond the research, we already see in China and the UK where the great firewall and the social lockdown are circumvented. Kids have more free time than adults and a lot more will to dedicate to finding ways around it.

There's an adage:

The internet detects censorship as damage and routes around it


The internet itself works against bans. Education and proper mental health funding for teens is vital.

I'll also state, beyond the social media not working, is the mental damage taking the social contact away from teens will cause. Not might, will. These teens have real friendships with people overseas or out of reach to them, that form proper social support networks. It's not only bad actors on the internet, otherwise it should be just turned off.

Practical example: my son keeps in contact with friends who've moved away (Aus->UK, US) through social media. Taking the social media away rips the friend groups apart. These friend groups are vital mental support groups and provide outlets that don't exist locally.

If you take nothing else away from this - a social media ban will cause immediate harm to teens. Serious harm.

Also, we've done this censorship dance before, it was beaten so quickly by Australian kids that I had to write an explainer

	s 47F  Thank you for your time All the best, s 47F
Response Method	Email
Submitted Date	15-Oct-2025 21:24 PM
Hermes ID	f1ca9136-e5f3-435a-b2f0-f8d44c332f4e

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.

From: s 47E(d) @esafety.gov.au
Sent: Monday, 12 January 2026 2:12 PM
To: s 47F
Subject: RE: Call to Block Grok AI [SEC=OFFICIAL]

OFFICIAL

Hello s 47F,

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,
eSafety enquiries
The 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.

From: s 47F
Sent: Sunday, 11 January 2026 6:06 AM
To: s 47E(d) @esafety.gov.au
Subject: Call to Block Grok AI

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

To Whom it may concern,

My name is s 47F and I am an Australian citizen s 47F. As a s 47F-year-old woman, I am highly concerned about the increasing use of non-consensual sexual deepfakes enabled by X's malignant and wholly unnecessary tool, Grok. This is of epidemic proportions in the U.S. and is rising at a lesser but nonetheless concerning rate in Australia.

On 28 April, 2024, the Prime Minister declared a 'national crisis' of violence against women. I believe that an integral mechanism to end this crisis is the regulation of generative AI, particularly Grok, as it enables violent ideology and violates women's autonomy.

Furthermore, with both anti-semitism and Islamaphobia on the rise, Grok increases these populations' vulnerability as it may be used to generate false images that, at their worst, may act as a false flag and incite public violence.

I urge the Australian Government to follow Indonesia's lead in banning Grok. Regulation and monitoring are insufficient as this leaves room for bad actors to inflict potentially irreversible violence. Our government is leading the way globally on eSafety with the new age restrictions, and this is the most sensible and secure next step.

Thank you for taking this into consideration. Please feel free to reach out to me with any updates or questions.

All the best,
s 47F

From: s 47E(d) @esafety.gov.au
Sent: Monday, 12 January 2026 4:54 PM
To: s 47F
Subject: Re: Concerns around use of Grok AI - xAI [SEC=OFFICIAL:Sensitive]
CRM:0367000000241

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Kind regards,
eSafety Enquiries
eSafety Commissioner
E s 47E(d) [@esafety.gov.au](mailto:s 47E(d)@esafety.gov.au)
W <https://www.esafety.gov.au/>



From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 2:04 PM
To: B
Cc: s 47E(d) @esafety.gov.au; Julie Inman Grant;
s 47F @mo.communications.gov.au; s 47F @aph.gov.au
Subject: RE: Shutdown or Complete Removal of Twitter/ X -The platform is spreading & distributing CSAM [SEC=OFFICIAL]

OFFICIAL

Hello s 47F,

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,
eSafety enquiries
The 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.

From: s 47F
Sent: Monday, 12 January 2026 6:16 PM
To: s 47F @mo.communications.gov.au; s 47F @aph.gov.au; Julie Inman Grant s 22 @eSafety.gov.au; s 47E(d) @esafety.gov.au
Subject: Shutdown or Complete Removal of Twitter/ X -The platform is spreading & distributing CSAM

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

Hi,

- Can you please review my request and respond with a clear decision by COB Thursday?

Considering the risks to minors and other individuals, I believe a fast and decisive response from the government and governing bodies is a more than fair expectation.

This shouldn't be controversial, as a citizen of Australia I am requesting that X/Twitter be shutdown or completely removed from operating in Australia due to spreading and distributing CSAM.

What has also been made clear is that the US is willing to use the apparatus of state to protect a private business that is contrevening local laws. This creates a clear risk to our nation's ongoing sovereignty.

Both in the past and currently X has violated both Australian laws and the laws of other sovereign states.

I am aware that Malaysia and Indonesia have blocked direct access to Grok but any individual who understands the platform structure can see that is pointless. Grok will still interact with offending accounts in other jurisdictions and the content will continue to be distributed.

This is not something that ethically should be deliberated.

Kind Regards

s 47F

--

Confidentiality Caution: The information contained in this email is confidential and is subject to copyright. It is intended solely for the addressee. If you received this by mistake please promptly notify me by email and then delete the email and destroy any printed copies. Thank you.

From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 2:12 PM
To: s 47F @icloud.com
Subject: RE: eSafety Contact Us Submission #ENQ-0024398 CRM:0244000002897 [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hello s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

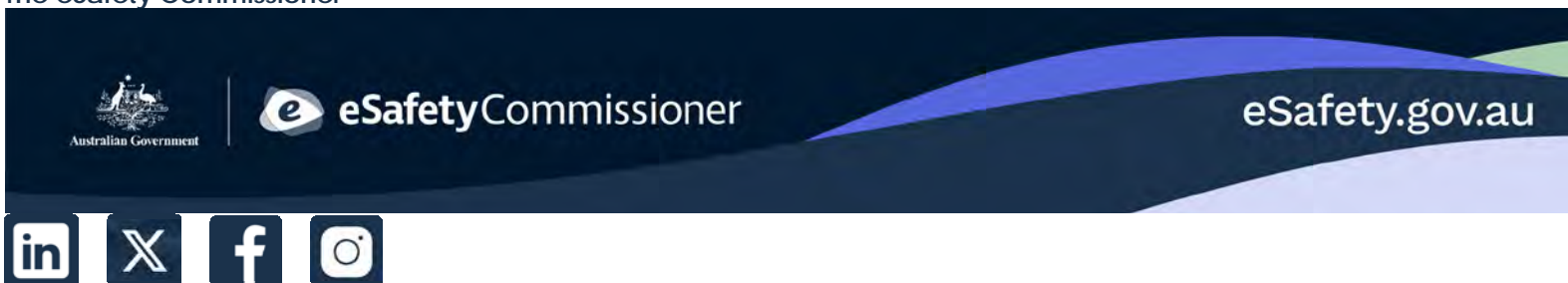
In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,
eSafety enquiries
The 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 -----

Enquiry ID	ENQ-0024398
Enquiry Type	Image Based Abuse
Due Date	18-Jan-2026 18:45 PM
Organisation	N/A
Name	s 47F
Email	
Phone	
Subject	Apple and Google's role in distribution of Grok and X
Details	Hello eSafety team, Referring to your statement from 9th January 2026, "eSafety raises concerns about misuse of Grok to generate sexualised content", I

respectfully request that your actions and the proportionality of your response, including enforcement actions, are informed not just by the volume of complaints you have received but by the abhorrence and volume of sexual abuse material being generated by Grok.

In addition, referring to an excerpt from a letter from US Senators to Tim Cook (CEO Apple) and Sundar Pichai (CEO Google) dated 9th January 2026, I encourage you to please consider relevance to Cth law and, if applicable, then write to Mr Cook and Mr Pichai to request the removal of Grok and X from their respective app stores.

https://www.wyden.senate.gov/imo/media/doc/letter_to_apple_and_google_on_removing_x_and_grok_from_app_store_192026pdf.pdf

“Dear Mr. Cook and Mr. Pichai:

We write to ask that you enforce your app stores’ terms of service against X Corp’s (hereafter, “X”) X and Grok apps for their mass generation of nonconsensual sexualized images of women and children. X’s generation of these harmful and likely illegal depictions of women and children has shown complete disregard for your stores’ distribution terms. Apple and Google must remove these apps from the app stores until X’s policy violations are addressed.

In recent days, X users have used the app’s Grok AI tool to generate nonconsensual sexual imagery of real, private citizens at scale. This trend has included Grok modifying images to depict women being sexually abused, humiliated, hurt, and even killed. In some cases, Grok has reportedly created sexualized images of children—the most heinous type of content imaginable. What is more, X has reportedly encouraged this behavior, including through the company’s CEO Elon Musk acknowledging this trend with laugh-cry emoji reactions. Researchers have also found a Grok app archive reportedly containing nearly 100 images of potential child sexual abuse materials generated since August, in addition to many other nonconsensual nude depictions of real people being tortured and worse. There can be no mistake about X’s knowledge, and, at best, negligent response to these trends.

Your app stores’ policies are clear. Google’s terms of service require apps to “prohibit users from creating, uploading, or distributing content that facilitates the exploitation or abuse of children” including prohibiting the “portrayal of children in a manner that could result in the sexual exploitation of children.” Apps that do not are said to be subject to “immediate removal from Google Play” for violations. Similarly, Apple’s terms of service bar apps from including “offensive” or “just plain creepy” content, which under any definition must include nonconsensually-generated sexualized images of children and women. Further, Apple’s terms explicitly bar apps from including content that is “[o]vertly sexual or pornographic material” ...”

Response Method	Email
Submitted Date	11-Jan-2026 18:42 PM
Hermes ID	28d42ac4-4ec0-464a-b2ea-b0534c3b9ae8

From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 4:17 PM
To: s 47F
Subject: eSafety Contact Us Submission #ENQ-0024188 CRM:0244000002794
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

Additionally, Australians can report illegal or restricted online content to eSafety. Australians experiencing image-based abuse, including AI-generated material shared without consent, can also report to eSafety at www.esafety.gov.au/report.

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety enquiries
The 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 and present.

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

From: eSafety Enquiries

Received: Sat Jan 03 2026 08:01:23 GMT+1100 (Australian Eastern Daylight Time)

To: Image Based abuse

Subject: eSafety Contact Us Submission #ENQ-0024188 [SEC=OFFICIAL:Sensitive] CRM:0244000002794

Enquiry ID	ENQ-0024188
Enquiry Type	Image Based Abuse
Due Date	10-Jan-2026 08:00 AM
Organisation	
Name	s 47F
Email	
Phone	
Subject	Regulatory gaps in AI image generation and image-based abuse on X
Details	<p>I am writing to raise a serious concern regarding the use of the Grok AI image generation system on the X (formerly Twitter) platform to create and publicly distribute non-consensual sexualised images of real women.</p> <p>Public reporting indicates from late December 2025 through early January 2026, users began widely using Grok to generate images that digitally remove or alter women’s clothing. These images have been produced in response to women expressing political, social, or</p>

personal opinions on the platform.

In multiple instances, Grok-generated images depicting women in states of nudity or sexualised exposure have been posted publicly on X, via the Grok X account or Grok-amplified posts, rather than solely through manual uploads by individual users. These images are not isolated or difficult to locate. They can be readily surfaced by using X's own search functionality, including the query "from:grok filter:media", where such content appears prominently and in high volume, effectively dominating the resulting feed.

The individuals depicted are real and identifiable, and the images are generated without their consent. Public posting on X constitutes distribution via a carriage service.

These images are being used explicitly to mock, humiliate, or silence women for engaging in lawful public speech. Under Australian law, non-consensual intimate or sexualised imagery, including AI-generated or synthetic images, constitutes image-based abuse. However, the current regulatory framework appears ill-equipped to address situations where:

- the imagery is generated automatically by a platform-deployed AI system
- the distribution occurs publicly and at scale
- responsibility is diffused between users and platform-operated systems

My concerns are that:

- X's deployment of Grok enables rapid, automated creation and wide distribution of image-based abuse
- Existing enforcement mechanisms appear reactive and complaint-driven, rather than preventative
- Platform accountability for AI-generated content remains unclear in practice despite clear harm
- Women are being subjected to sexualised humiliation as a response to lawful public participation

I am seeking clarification on whether the government is considering stronger regulatory obligations for platforms such as X when deploying AI image generation tools, including:

	<ul style="list-style-type: none"> - clearer liability for automated or AI-mediated distribution of abusive imagery - mandatory safeguards to prevent non-consensual sexualised image generation - faster enforcement mechanisms where abuse is systemic rather than individual <p>I would appreciate information on any current or planned government action, inquiries, or regulatory reforms addressing AI-generated image based abuse on major platforms.</p> <p>Thank you for your time and attention to this issue. I look forward to your response.</p> <p>Kind regards, s 47F</p>
Response Method	Email
Submitted Date	03-Jan-2026 00:54 AM
Hermes ID	25d79ac9-f14e-4a0f-89ab-2f989e28a8d8

From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 4:21 PM
To: s 47F
Subject: RE: eSafety Contact Us Submission #ENQ-0024322 CRM:0244000002854
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety enquiries
The 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 and present.

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

From: eSafety Enquiries

Received: Thu Jan 08 2026 08:40:42 GMT+1100 (Australian Eastern Daylight Time)

To: Image Based abuse

Subject: eSafety Contact Us Submission #ENQ-0024322 [SEC=OFFICIAL:Sensitive] CRM:0244000002854

Enquiry ID	ENQ-0024322
Enquiry Type	Image Based Abuse
Due Date	15-Jan-2026 08:40 AM
Organisation	
Name	s 47F
Email	
Phone	
Subject	Use of Grok to generate nude photos
Details	<p>Good morning,</p> <p>I am writing to you as a concerned s 47F</p> <p>I am deepy disturbed and angry about the use of Grok on X to allow men to generate non-consensual nude images of women and children, and I would like to know if the eSafety commissioner has plans to challenge X to fix this. I recently read a response from eSafety to the Guardian that using Grok to nudify images of children do not meet the threshold of generating child abuse material. Am I correct in this understanding? Can you please explain how this is the case, and if there is a plan to review the standards to keep up?</p>

Response Method	Email
Submitted Date	08-Jan-2026 08:38 AM
Hermes ID	1ee16835-ac0e-4b7c-98f7-60323eb634b1

From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 4:22 PM
To: s 47F
Subject: RE: eSafety Contact Us Submission #ENQ-0024222 CRM:0244000002809
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety enquiries
The 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 and present.

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

From: eSafety Enquiries

Received: Mon Jan 05 2026 10:45:18 GMT+1100 (Australian Eastern Daylight Time)

To: Image Based abuse

Subject: eSafety Contact Us Submission #ENQ-0024222 [SEC=OFFICIAL:Sensitive] CRM:0244000002809

Enquiry ID	ENQ-0024222
Enquiry Type	Image Based Abuse
Due Date	12-Jan-2026 10:45 AM
Organisation	N/A
Name	s 47F
Email	[Redacted]
Phone	
Subject	Twitter/X - use of AI to generate non-consensual images
Details	<p>Hello there,</p> <p>In recent days there have been numerous instances of Twitter/X's chatbot 'Grok' being asked to modify photos of real people to put them in bikinis/lingerie. In some instances, this has been to images involving children.</p> <p>I would like to know whether the Commissioner is intending to take any action.</p>
Response Method	Email

Submitted Date	05-Jan-2026 10:44 AM
Hermes ID	00a05a55-5b43-48c1-8d5c-05b46b0f2b3a

From: s 47E(d) @esafety.gov.au
Sent: Tuesday, 13 January 2026 4:23 PM
To: s 47F
Subject: RE: eSafety Contact Us Submission #ENQ-0024237 CRM:0244000002817
[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Dear s 47F

Thank you for your enquiry to the eSafety Commissioner.

eSafety remains concerned about the use of the generative AI system Grok on X to generate content that may sexualise or exploit people, particularly children.

eSafety will use its powers, including removal notices, where appropriate and where material meets the relevant thresholds defined in the Online Safety Act.

X, Grok, and a wide range of other services are also subject to systemic safety obligations to detect and remove child sexual exploitation material and other unlawful material as part of Australia's world-leading [industry codes and standards](#).

eSafety has written to X seeking further information about the safeguards in place to prevent Grok's misuse on its service and to comply with these obligations.

If you think a service is not complying with an industry code or standard, you can make a complaint to eSafety using our Online Safety Codes and Standards complaint form. The complaint form is available here: [Online Safety Codes and Standards complaints | eSafety Commissioner](#).

Additionally, Australians can report illegal or restricted online content to eSafety. Australians experiencing image-based abuse, including AI-generated material shared without consent, can also report to eSafety at www.esafety.gov.au/report.

The safety of generative AI services and features is a key regulatory priority for eSafety. eSafety has already taken enforcement action in 2025 in relation to some of the "nudify" services most widely used to create AI child sexual exploitation material, leading to their withdrawal from Australia ([eSafety action prevents services "nudifying" Australian school children](#)).

In addition, eSafety expects all covered services to take reasonable steps to comply with the [Basic Online Safety Expectations](#), including the expectation to proactively minimise the extent to which material or activity on the service is unlawful or harmful to children.

eSafety is also engaging closely with international child protection organisations and online safety regulators, who have identified similar emerging patterns involving generative AI tools.

These developments reinforce the importance of strong safeguards and [Safety by Design](#) measures to prevent the misuse of generative AI, particularly where children are involved.

Thank you for bringing your concerns to our attention. We hope this information is helpful.

Regards,

eSafety enquiries
The 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 and present.

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

From: eSafety Enquiries
Received: Mon Jan 05 2026 18:10:29 GMT+1100 (Australian Eastern Daylight Time)
To: Image Based abuse
Subject: eSafety Contact Us Submission #ENQ-0024237 [SEC=OFFICIAL:Sensitive] CRM:0244000002817

Enquiry ID	ENQ-0024237
Enquiry Type	Image Based Abuse
Due Date	12-Jan-2026 18:10 PM
Organisation	Independent
Name	s 47F
Email	
Phone	
Subject	Uptake in AI
Details	As I'm sure you're aware, AI chatbots available in Australia currently allow people to upload any photo of someone and request for the clothing to be removed. I understand this is difficult to completely prevent, but measures such as regulations, legislation, and technical blocks need to be put in place to reduce the ease and accessibility of this. I look forward to hearing your thoughts and what

	actions are currently being taken by the Australian Government to protect citizens, namely women and minors, from this exploitation. Thank you.
Response Method	Email
Submitted Date	05-Jan-2026 18:08 PM
Hermes ID	28e5813f-502e-445d-bea0-95a1483fcb18

Complaint

CYR-0744138

Created On
10/01/2026 6:38 PM

Complaint Status
Not Actionable

Assigned To
s 22

Response Required
No

Summary

Date Received
10/01/2026 6:38 PM

Complaint Status
Not Actionable


Source Type
CYR

Date Finalised
13/01/2026

Assigned To
s 22

Derived
No

Title:
NA – Not class 1 or class 2 material. The material at the URL provided is unlikely to be class 1 (RC) or class 2 (adult content) material under sections 106 and 107 of the OSA.

 Screenshot_13-1-2026_92218_x.com.jpeg
s 22 13/01/2026 9:22 AM

Complainant

Anonymous Complaint Yes
Australian Resident Yes

Police Involved No
Education Provider No

Complainant

Repeat Complainant
No

Complainant Reason
 Child sexual abuse / child abuse / Paedophile activity

Response Required No
Response Method

Submission

Method Received
Web Form

Presentation Type
Social media

Device Type
Mobile Phone

Device Name

Remote IP Address

Access Information

Additional access instructions

Users are able to create and post sexually explicit AI created media depicting other users (from photos posted on the platform). This includes creating and sharing sexually explicit images of children.

Access Username

Access Password

Related Entities

URL	Type	Investigation Id	Status	Investigated Loc
s 47E(d)	Complained Social Media Se			

1 - 1 of 1 (0 selected) Page 1

S...	Investigation Id	Status	Investigated Loca
0 - 0 of 0 (0 selected) Page 1			

Response

Response/RFI Templates

Name	Created On	Status
No Complaint Response records are available in this view.		

0 - 0 of 0 (0 selected) Page 1

Email Activities

Date Sent/Received	From	To	Subject	Status F
No E-mail records are available in this view.				

0 - 0 of 0 (0 selected) Page 1

Assessment

Content Tags

Name
Grok

1 - 1 of 1 (0 selected) Page 1

[Redacted content]