Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

eSafety Key Statistics

Investigations stats - s 22					
1 July 2025 – 31 March 2026	**Adult Cyber Abuse**	**Cyberbullying**	**Image-based Abuse**	**Illegal and Restricted Content**	**Totals**
Complaints received (% change from PY[1])	4,239 (+66%)	2,741 (+10%)	6,664 (+39%)	21,142 (+48%)	34,786 (+44%)
% that don't meet legislative threshold	96%	73%	29%		
# complaint notifications[2])	10	155	911	532	1,608
# of SPNs	84	248	23	0	355
# formal removal notices	7 issued, 7 removed	3 issued, 1 removed	0 issued, 0 removed	48 issued, 23 removed	58 issued, 31 removed
# of link deletion notices sent for class 1	N/A	N/A	N/A	0	0
# of remedial directions	N/A	N/A	1	N/A	1
# formal warnings	0	1	0	0	1
Top 3 sub-categories by volume	Defamation (43%)	Nasty comments/ serious name calling (36%)	Sexual extortion (49%)	Child sexual abuse / child abuse / Paedophile activity (67%)	
	Nasty comments/ name calling (24%)	Offensive/ upsetting pictures and/or videos (24%)	Child sexual exploitation (12%)	Extreme, offensive or adult content (13%)	
	Doxing (10%)	Unwanted contact (9%)	Posted online (8%)	Sexually explicit (7%)	
% of complainants who identify as gender diverse	1.3%	1.6%	1.2%	N/A	

No infringement notices were issued under the complaint schemes in 1 July – 31 March period

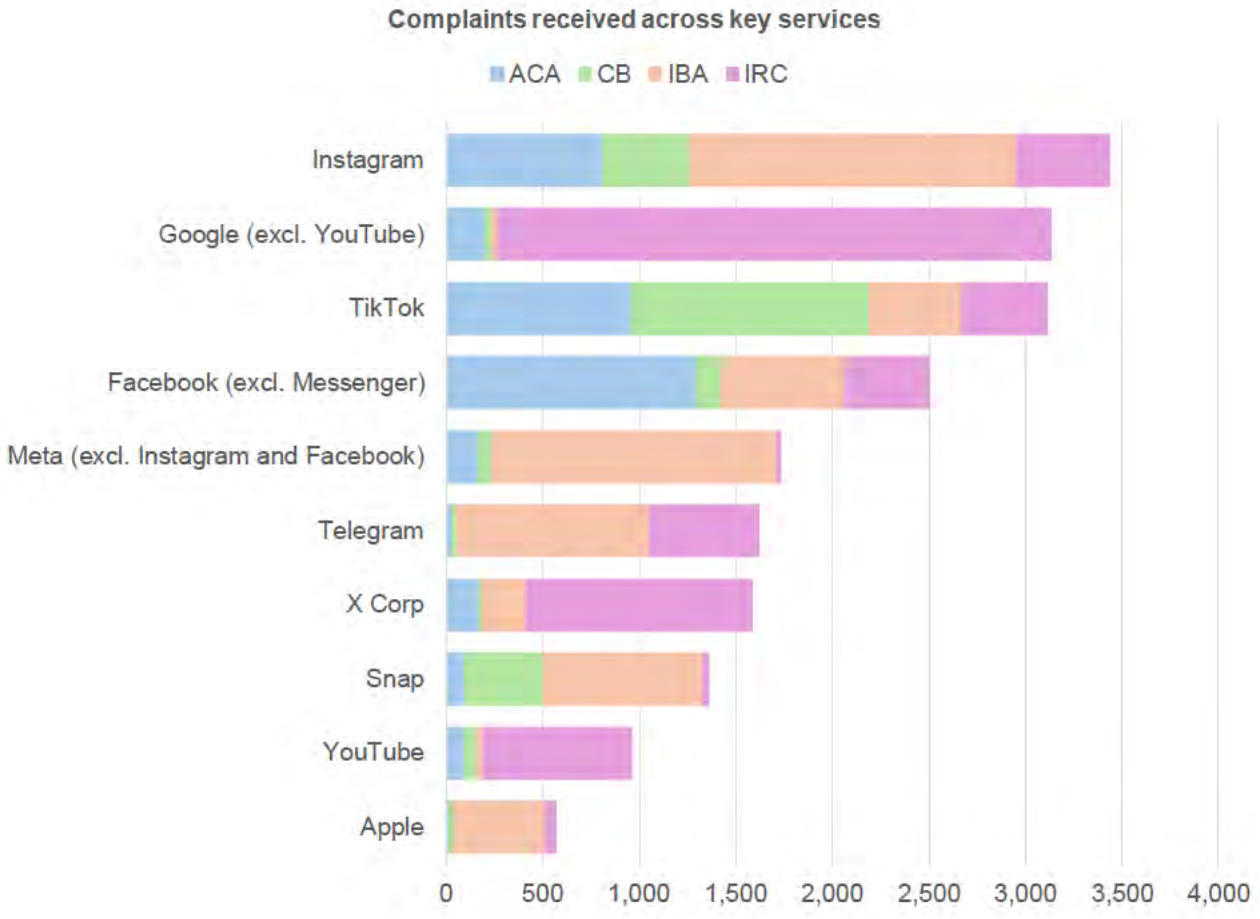
[1] Compared to 1 July to 31 March 2025.
[2] A complaint notification may include multiple urls

Topical issues under the complaint schemes	
TVEC	Makes up 7% of complaints received under our IRC scheme. This financial year saw a 498% increase in number of complaints made. 133 investigations completed each containing content that had been classified as RC. A refinement of assessment processes means complaints are only progressed to investigations where the content is sufficiently serious has resulted in a significant decrease in the number of investigations.

Online hate	Race-related Adult Cyber Abuse Complaints
	
	• eSafety received 18 complaints involving religious or race-related abuse:
	  • 4 antisemitic
	  • 10 Islamophobic
	  • 2 targeting Aboriginal/Torres Strait Islanders
	  • 2 other race-based discrimination
	
	No antisemitic complaints met the adult cyber abuse threshold.
	
	Gender related Adult Cyber Abuse Complaints
	
	In 1 July 2025 – 31 March 2026, the adult cyber abuse scheme received 6 complaints relating to gender.
	
	Child Cyberbullying
	
	• eSafety received 3 complaints that involved belief-based abuse
	• None of these complaints met the cyberbullying threshold
	• 7 complaints were received relating to the complainant's gender
	• 3 of these complaints met the cyberbullying threshold
	• 51 complaints were received relating to the complainant's race/ethnicity
	• 23 complaints met the cyberbullying threshold

CSAM	Comprised 12% of IBA complaints (9% of total reports in July – March 2025). 75% increase in number of CSAM reports made compared to July – March 2025. Comprised 67% of IRC complaints (79% in July – March 2025). 26% increase in number of complaints made compared to July – March 2025. 3,308 investigations were completed that contained Class 1 (RC) content. Noting the investigation numbers are commonly higher than the complaints numbers due to the amount of own motion investigations that are instigated following the detection of CSAM. For example, a single complaint may contain multiple URL's of CSAM which correlate to multiple own motion investigations. As with TVEC complaints, a refinement of assessment processes means complaints are only progressed to investigations where the content is sufficiently serious has resulted in a significant decrease in the number of investigations.

Complaints across key services (IBA and IRC figures are based on keyword searches and may include false positives (or exclude false negatives))				
Service	**ACA**	**CB**	**IBA**	**IRC**
Google (excl. YouTube)	204	32	34	2,865[3]
Snap	95	411	825	33
Tik Tok	958	1,230	477	451
Apple	16	24	472	61
Meta	167	71	1,474	24
Instagram	811	456	1,682	491
Facebook (excl Facebook Messenger)	1,297	127	638	443
You Tube	93	65	34	772
X Corp	173	13	225	1,179
Telegram	32	24	997	567



[3] Caution should be had in interpreting this figure as it includes results for google searches where the content is ultimately on another service

Comms stats – Awareness and reach Performance Q1-Q3 2025/26 (comparison is vs same period in 2024/25)		
1 July 2025 – 31 March 2026	**eSafety.gov.au**	**BeConnected.gov.au**
Webpage visits	**+ 11.8 million users** (+84%) Of this traffic: • 74.7% was organic traffic • 13% was direct traffic • 3.8% was paid traffic *Source: Google Analytics*	**+ 309K users** (-19%) Of this traffic: • 42.5% was direct traffic • 41.6% was organic traffic • 8.0% was email traffic • 5.9% was referred traffic *Source: Google Analytics*
Web resource downloads	+225K downloads *Source: Google Analytics*	+18K downloads *Source: Google Analytics*
Email activity	+1.459M emails sent (+50%) from 143 email campaigns (+18%) *Source: MarComms reporting - per Monthly MO Reports*	• Be Connected learner and subscriber community has grown to 47k (+17.07%) *Source: Campaign Monitor Reporting*
	More than 90,000 subscribers at end March 2026 (+47%) *Source: MarComms reporting - per Monthly MO Reports*	• +34K Be Connected learner newsletter subscribers (+ 4.7%) • +13K Be Connected newsletter only subscribers (+ 45.94%) *Source: MarComms reporting - per Monthly MO Reports*
Media stats	eSafety issued 44 media releases and statements *Source: eSafety website*	
	Over 22,000 media mentions *Source: Isentia Reporting*	
	Estimated media reach of more than 443m (audience), or media Advertising Space Rate (ASR) of more than $273m. *Source: Isentia Reporting*	
Social media stats	Over 99,000 social followers at March 2026 (15% growth across Jul 2025 to Mar 2026, though the figure is lower as eSafety's X account is no longer in active use) *Source: MarComms reporting - per Monthly MO Reports*	
	493 social media posts published	

	4.3m post impressions in Jul 2025 to Mar 2026 (1.36m in Jul 2024 to Mar 2025, 214% increase)	
Events delivered	The Commissioner delivered more than **30 external engagements, reaching an estimated 5,500 attendees (in-person and online).** *Source: JIRA Commissioner Engagement Reporting*	
Awareness activities	Across the second half of 2025, eSafety reached **close to 4 million Australians** through targeted digital education and awareness initiatives, driving **more than 190,000 users** to trusted safety information and support. This included **1.6 million reach** to parents and carers, generating **4,500+ webinar registrations**, and tens of thousands of young people accessing help on tech-based abuse and coercive control. From 15 May to 17 July 2025 eSafety delivered an **awareness campaign** aimed at **young people aged between 18 to 24** years and their support networks, to raise awareness of **tech-based coercive control**, to educate them on specific behaviours that form part of a broader pattern of control and to empower them to take action. The channels included paid search, Meta, TikTok, programmatic display, and a paid partnership with The Daily Aus. Key results: - Reached approximately 824k - 712k video ad views - 16.5k unique users to eSafety's campaign landing page. From 6 July to 21 August 2025 eSafety executed a campaign aimed at **parents and carers** to drive registrations to our **free webinar program**. The channels included paid search, Meta, and programmatic display. Key results: - 1.6 million unique reach - 55k users to the webinar pages - Over 4.5k registrations. From 22 October to 28 November 2025 eSafety delivered an **awareness campaign** aimed at **young people aged 14-18**, to raise awareness of the subtle and often hidden **tech-based abuse tactics used by abusive caregivers** against children and young people, and to guide them to the eSafety website to find support resources. Channels included gaming platforms, digital display, Meta, Snapchat, TikTok and Spotify. Key results: - Reached approximately 1 million - Over 53k users to the campaign landing page. From the period 1 July 2025 to 31 March 2025, eSafety's paid search campaigns have driven over 200,000k users to our website, resulting in over 750k page views, and close to 20k web resource downloads.	

Education Prevention and Communities- training attendees						
	Gender and tech	**Primary school children**	**Educators**	**Parents and carers**	**Seniors**	**Support services and broader community**
Attendees at webinars/ presentations	1,937	70,041	17,105	7,576	1,937	7,981
Audiences include:	*Domestic, family and sexual violence workers and other gendered presentations including Social Media Self-Defence*	*Virtual Classrooms for Primary school aged children (years 3-4)*	*National Student Wellbeing Officer professional learning program, teachers and support staff, Pre-service teachers, tertiary sector.*	*Parents and carers*	*Senior Australians as part of the BeConnected Program*	*Health, wellbeing and support services government agencies, corporate audiences, sporting and other community groups (eg disability, First Nations, LGBTIQ+)*

Trusted eSafety Providers				
	Students	**Parents & Carers**	**Educators**	**Total audience**
Reach	1,374,726	34,400	53,902	1,625,668

Corporate top line stats – Jason Armstrong				
Staffing numbers at 30 April 2026	APS FTE	236	Under the Strategic Commissioning Framework, eSafety has converted approximately **27** positions from contractors to ASL (24-25 and 25-26)	
	Contractors FTE	20		
	Total	**256**		
2026-27 Budget As per the 2026-27 PBS	Departmental	$66.5m		
	Administered	$3.5m		
	Total	**$70.0m**		
SMAA funding received	2024-25	2025-26	2026-27	2027-28
	$3.8m	**$16.2m**	**$13.3m**	**$12.4m**
External legal expenditure at 30 April 2026	2024-25 FY	2025-26 YTD	2025-26 expense excludes costs paid to X Corp re Wakeley case of $0.624m.	
	$1.018m	**$1.889m**		
Travel expenditure at 30 April 2026	Domestic travel 2024-25 FY	Domestic travel 2025-26 YTD	Overseas travel 2024-25 FY	Overseas travel 2025-26 YTD
	$0.670m	**$0.446m**	**$0.349m**	**$0.152m**

AAT results – selected examples			
Age Verification technologies – 27 vendors participated, TRL range 8-9.			
Vendor / Technology name	**Technology type**	**TRL**	**Comments**
Austroads	Enables verified credentials and selective age attestations via government issued ID (Driver's licences)	8-9	Austroads manages the National Exchange of Vehicle and Driver Information System (NEVDIS) and is working on Mobile Driver Licence (mDL) standards. Relying party queries a government API or wallet service for a "match/no match" check - no DOB is returned
AgeChecked	Uses data matching, credit reference checks, electoral rolls, facial age estimation, document verification with liveness detection and adult-linked credit card checks in a cascading process	9	
Australian Payments Plus - ConnectID	Relies on banks' KYC-verified date of birth to return yes/no age assertions;	9	Peer to peer exchange model ensures that no Personal Identity information is ever visible to ConnectID; only consented minimal data (e.g. 'over 18') is shared.
LexisNexis - IDVerse	Uses AI for real-time age verification via biometric face matching, liveness detection and OCR	9	
Luciditi	System includes facial age estimation, document verification via selfie-ID match, NFC passport reading and open banking or telco records, with fallback to a reusable digital ID app.	9	Verified users across 13+, 16+ and 18+ thresholds with high accuracy.
Age Estimation technologies – 13 vendors participated, TRL range 7-9			
Yoti	Uses facial age estimation either on-device or at the edge.	9	Certified for privacy and security compliance, GDPR aligned; does not store images. Mean Absolute Error (MAE) values under 2 years for ages 13–20. 80% of users reported being either satisfied or very satisfied with the experience.
IDMission	Facial age estimation	8	Lab and school testing demonstrated MAE above 4.5 indicated low precision and high false positive rates. Trial suggested further validation needed before commercial deployment. **NB**: Demonstrates that the accuracy varies by vendor – not just by technology type.
Persona	Uses facial estimation with optional ID fallback	8	MAE ranged from 0.86 to 3.31 across different cohorts

Needemand - BorderAge	Uses hand gesture dynamics, captured via a device's camera; does not use biometric or identity data	8	Gesture based preferred by many mystery shoppers due to non-invasive feeling.
Age Inference technologies – 9 vendors participated, TRL range provided 5-8			
Verifymy	Age inference using metadata, email domains and app interaction context	7	While operational, its age inference capability is narrower and more targeted (e.g. "likely under 13") and evidence suggests it is part of layered access control.
AgeChecked	Integrated with payment processors to test users' ability to initiate a zero-dollar authenticated credit card transaction, with verification via one-time passcode.	*	Since credit cards are legally restricted to those 16+ in Australia (as additional cardholders), a successful result offered a medium confidence, binary signal of being over 16 at least.
Yoti	Behavioural and contextual age inference – eg. account metadata (age of account, frequency of use), content engagement patterns, device and browser context.	*	Triggers fallback to facial age estimation where confidence in inference result is low.

** Yoti and AgeChecked's inference products not given separate TRL to vendors bundled solutions.*

All systems assessed/tested in the trial were TRL 7 and above. Some emerging approaches (TRL <7 where discussed, but unable to be tested).

TRL 9	**System Proven and Ready for Full Commercial Deployment**: Actual system proven through successful operation in an operating environment, ready for full commercial deployment.
TRL 8	**System Incorporated in Commercial Design**: Actual system/process completed and qualified through test and demonstration (pre-commercial demonstration)
TRL 7	**Integrated Pilot System Demonstrated**: System/process prototype demonstration in an operational environment (integrated pilot system level)

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: BOSE (Expectations)

Talking Points

- Meaningful transparency is essential to drive change. Without access to information from industry participants, eSafety cannot fulfil its functions and industry cannot be held accountable. These processes shine a light on industry practice and drive change.
- The Expectations have been in effect since early 2022. Since then, eSafety has given **27 non-periodic notices, 8 periodic notices**, **11 information requests**, and published **8 transparency reports**.
- Our most recent report (published 24 March 2026) sheds a light on the safety measures four AI Companion services have in place to protect Australian children.
- We have also recently given notices to four online game providers, seeking information about the steps they are taking to protect children from child sexual exploitation and abuse, radicalisation and bullying on their services.
- We will soon publish the third periodic report looking at the steps mainstream providers of online services are taking to address child sexual exploitation and abuse on their platforms. Our previous 2 reports indicate providers are taking some steps to improve safety but should take further steps to detect new CSEA, address livestreaming of CSEA and stem the proliferation of sexual extortion of children and adults.

Key Issues

Non-periodic notices

- Non-periodic notices focus on steps providers are taking to meet the Expectations during a particular period. Our approach is to focus on specific Expectations and issues of high harm.

<u>Gaming services (notices given to Roblox, Minecraft, Fortnite and Steam in Apr 2026)</u>

- eSafety's most recent non-periodic notices were given in **April 2026 to four online game providers – Roblox, Minecraft, Fortnite and Steam.**
- Online gaming services are excluded from the SMMA as they do not carry the same risks associated with social media features such as recommender systems and endless scroll.
- However, Roblox, Minecraft and Fortnite do have metaverse- or sandbox-style features, which have been found to heighten the risks of grooming, sexual extortion and radicalisation. In such cases, gaming platforms can serve as a place of first contact between children and offenders, before moving to more encrypted messaging or 'game-adjacent' services.
- The notices therefore seek information about the safety measures these services have in place to protect children from child sexual exploitation and abuse, such as grooming and sexual extortion, as well as radicalisation, cyberbullying and online hate.
- The notices cover the period 20 March 2025 to 20 March 2026. This covers Roblox's introduction of age-verified chat, which was rolled out in Australia on 3 December 2025.
- eSafety expects to publish a summary of the information obtained from these notices in September this year.

Contact: s 22
Phone:

Cleared by: s 22, Executive Manager, ICE
Date: 15/04/2026

AI companion services (report re Character.AI, Nomi, Chai and Chub published in Mar 2026)

- eSafety recently published the findings from notices given to **AI Companion services – Character.AI, Nomi, Chai and Chub**. These notices sought information about measures to mitigate CSEA, self-harm, suicide, and pornography, which includes sexualised role play.
- Key findings from this report were:
    - **Children were able to access adult features:** None of the providers had robust age verification measures, relying instead on app store ratings or self-declaration at signup.
    - **Self-harm support lacking:** Chai, Chub AI, and Nomi did not direct users to mental health or crisis support when self-harm was detected in user-prompts.
    - **Failure to check for harmful content:** Chub AI and Nomi did not monitor inputs or outputs across all relevant text, image and video AI models for unlawful or potentially harmful material. Chai failed to check outputs across all relevant models.
    - **Limited trust & safety staffing:** Nomi and Chub had no dedicated trust & safety staff.
    - **No reporting of CSEA attempts:** Chai and Nomi did not advise users of the criminality of prompting for child sexual exploitation and abuse material, nor did they report child sexual exploitation and abuse material to enforcement authorities or to child protection organisations like the US National Center for Missing and Exploited Children (NCMEC).
    - **Failure to red-team:** Chub AI and Nomi did not conduct red-teaming (i.e., testing for vulnerabilities, limitations or potential for misuse) across all models used to provide their service. This can increase the risk of illegal or harmful material being produced.
- The report also included findings from our survey of 1,950 children aged 10 to 17 in Australia. The results of this survey show that AI companions and AI assistants are already a common part of their lives. **79% of children told us they had used either an AI companion or AI assistant.** While the majority of these children had used an AI assistant, **8% said they had used an AI companion**. We estimate this **represents around 200,000 children** in Australia.

Periodic notices (report 1 published in Aug 2025; report 2 in Feb 2026; report 3 forthcoming)

- Periodic notices enable eSafety to understand compliance with the Expectations over time.
- The first round of periodic notices was given in July 2024 to **Apple, Discord, Google, Meta, Microsoft, Snap, Skype** and **WhatsApp.**
- The notices require reporting every 6 months over 2 years on compliance with the Expectations, focusing on CSEA including grooming, and sextortion of children and adults.
- eSafety published the first periodic report in Aug 2025, and the second in Feb 2026. eSafety expects to publish the third report in July 2026.
- Key takeaways from report 2 include:
    - Mainstream platforms are taking some steps to improve the safety of their services including improving or expanding the tools they use to detect CSEA. Examples include:
        - **Microsoft** - reported **expanded use of hash matching** for known CSEA images in email attachments in Outlook, and images and videos in OneDrive.
        - **Discord** - reported it **started hash matching** to detect known CSEA videos.
        - **Meta** - used **more sources** for its lists of terms and language indicators to detect sexual extortion (NCMEC and Thorn).
        - **Skype** - implemented proprietary **program for calls** in certain regions, including Australia, for high-risk users. If CSEA is detected, the video is disabled.
        - **Google joined Take it Down** – a global hash-matching service operated by NCMEC which helps remove and prevent the distribution of online nude, partially nude or sexually explicit photos and videos of children under 18.
        - **Apple** - continued development of its **Communication Safety** feature (and Sensitive Content Warning) with the aim of expanding to more of its services.
    - **Despite these improvements, significant safety gaps remain** to:
        - address online CSEA / CSEA **livestreaming**;
        - detect **new CSEA**; and
        - stem the proliferation of **sexual extortion** of both children and adults.

Information requests

- In addition to notices, eSafety may also obtain information from providers under section 20 of the BOSE Determination, which sets out the expectation that providers will provide certain information to the Commissioner within 30 days on request. Information requests are not backed by civil penalties, but can result in a ‘statement of non-compliance'.
- This information-gathering mechanism was used to collect information from 7 providers in late 2024 in relation to age assurance and informed eSafety’s **Behind the Screen report** published in February last year, which provided important insights to inform our work on the SMMA.
- eSafety has also recently used this information-gathering mechanism to obtain monthly active user data from **online game providers**.

Difficult Questions

If providers don’t meet Expectations, why haven’t you taken enforcement action?

- The Basic Online Safety Expectations are about transparency rather than enforcement.
- The periodic notices are intended to keep the pressure on these companies by requiring them to answer the same set of questions over two years (until August 2026).
- eSafety intends to publish regular transparency reports following responses to these notices. These reports serve to incentivise meaningful safety improvements across the technology sector and hold companies accountable for protecting their most vulnerable users. They also demonstrate improvements being made and tech solutions available to keep users safe.
- Where we identify ongoing safety gaps, eSafety considers alternative enforcement options, including the codes and standards which require providers to detect, disrupt and deter CSEA.

If GenAI providers are not meeting the Expectations what action will you take?

- While the Expectations are not enforceable, the Age Restricted Material Codes are enforceable and took effect on 9 March 2026 and apply to Gen AI Companions. Requirements include:
    - **Design for safety** to prevent illegal and harmful content.
    - **Age assurance on highest-risk features** so only adults can access functions that could generate high-impact material, such as self-harm and online pornography.
    - **Extra protections on medium-risk services without age assurance** to prevent children generating harmful or age-inappropriate content.
    - **Quick and consistent moderation and escalation**, including working with police.
    - **Clear ways for users to report issues and seek help**, plus regular risk assessments.
    - **Regular testing and review**, with documented results and improvements over time.
- eSafety will use the full range of our powers to ensure compliance and deter non-compliance. This can include seeking penalties from the Federal Court of up to A$49.5m.

Why didn’t you send notices to Grok and ChatGPT?

- eSafety takes a range of factors into account in determining which services to issue notices to including Australian usage, publicly available safety information, opportunity to enhance a services understanding of the Australian regulatory regime. For non-periodic notices eSafety generally considers four notice recipients is appropriate – issuing to a larger number delays review and reporting times.
- eSafety has previously given a notice to X seeking information on Grok’s safety measures to prevent pro-terror material. X challenged that notice in the Administrative Review Tribunal (ART), and the Tribunal remitted the decision to eSafety.

- It is open to eSafety to issue further notices to additional companies with AI capabilities in due course to continue building a picture of online safety measures across the industry.
- In addition to BOSE periodic and non-periodic notices, eSafety also has powers under the Online Safety Act to investigate allegations of non-compliance with mandatory Codes and Standards.

Why give a notice to Chub AI when it's not available in Australia?

- Prior to issuing these Notices, the Chub service was available to Australians.
- During eSafety's engagement with Chub AI Inc. about specific expectations under the BOSE to protect children, it decided to withdraw its service from Australia on 1 October 2025. Given the notice process was already on foot and we had no certainty Chub AI would not reintroduce its service to Australia, we considered it appropriate to seek a response from Chub AI.

Why aren't online games like Roblox included in the social media minimum age?

- The social media minimum age restrictions are focused on preventing children under 16 from having accounts on age-restricted social media platforms.
- The age restrictions aim to protect young people from risks and harms that come from social media platform design features that encourage users to spend more time on platforms, such as algorithms and recommender systems, and risk exposing young people to harmful content.
- Age restrictions apply to social media platforms that meet specific conditions, unless they are excluded based on criteria set in out in legislative rules made by the Minister. The Department is best placed to answer questions about those rules.
- Services that have the sole or primary purpose of enabling end-users to play online games with other end-user are among the types of services that have been excluded under the rules. Even without the exclusion, some online games may not meet the definition of an ARSMP depending on the features of the particular service. At this time, eSafety has assessed Roblox as having the sole or primary purpose of enabling end-users to play online games. It is possible over time, should Roblox continue to change its features and functions or the way end-users use the service changes, it could become an ARSMP.

How have you dealt with non-compliance with reporting requirements?

- eSafety has taken action in relation to 4 notices given to 3 companies:
  - **X Corp. – 1 x Infringement Notice and 2 x Service Provider Notifications**
    - **Infringement Notice** of $610,500 & **Service Provider Notification** to X Corp. re: February 2023 CSEA Notice. X Corp. applied for judicial review, which was dismissed in October 2024 and dismissed again on all grounds with costs on appeal to the Federal Court. eSafety filed civil penalty proceedings in December 2023 following non-payment of the infringement notice, which are ongoing.
    - **Service Provider Notification** to X Corp. in January 2024 for giving inaccurate and incomplete response to June 2023 Online Hate Notice.
  - **Google – 1 x Formal Warning**
    - Formal Warning to Google for failure to adequately answer some questions in the February 2023 CSEA Notice.
  - **Telegram – 1 x Infringement Notice**
    - Infringement Notice of $957,780 for failure to respond to the notice by the deadline. Telegram's response was provided to eSafety 160 days after the due date. Telegram did not pay the infringement notice. Telegram applied to the Federal Court for judicial

review of the notice, claiming the legal entity to which eSafety gave the Notice (i.e. Telegram FZ LLC) is not the legal entity that provides the Telegram service.

- Telegram has discontinued the proceedings.

Are your enforcement powers ineffective?

- The 2024 review of the Online Safety Act recommended strengthening our powers, which government and eSafety support.
- We have seen improvements in online safety through the actions we have taken to date and the progress shown in the latest transparency report is evidence of this.
- While the Expectations themselves are not enforceable, the requirement to respond to a transparency notice is enforceable, with a maximum penalty of $825,000 per contravention.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Social Media Minimum Age - Compliance

Talking Points

- We're now five months into implementation. Overall, while there has been a reduction in the number of social media accounts held by Australians under 16 years, a substantial number of children under 16 years continue to hold accounts.
- As outlined in eSafety's compliance update published on 31 March 2026, eSafety has observed poor practices by some platforms, giving rise to compliance concerns.
- Accordingly, eSafety is investigating the providers of Facebook, Instagram, Snapchat, TikTok and YouTube for potential non-compliance. We are also actively engaging with these platforms to achieve uplift, and in some cases, we are seeing improvements being implemented.
- eSafety aims to finalise at least some of these investigations and make a decision about any enforcement action around the middle of 2026, however these timeframes are dependent on a range of factors, including the quality of the information we obtain from platforms, any improvements platforms are making and any further evidence we need to obtain to establish a breach of the law.
- While we will continue to be as transparent as possible, there are some details we are unable to share while investigations are underway, as doing so would or might reasonably be expected to prejudice eSafety's investigations and any potential future enforcement action.

Key Issues

- The SMMA obligation requires providers of age-restricted social media platforms to take **reasonable steps** to prevent Australian children under 16 years from having accounts on their platforms. Whether a platform has taken reasonable steps is contextually dependent and requires a review of the regulatory landscape and business circumstances in tandem; it is not a prescriptive test with a one-size-fits-all approach but instead requires a review of all steps taken in totality.
- While platforms have taken some steps to comply with the SMMA, eSafety has identified a range of **poor practices** which raise concerns about compliance.
- As a result, eSafety is investigating potential non-compliance by **Facebook, Instagram, Snapchat, TikTok and YouTube**, with decisions on possible enforcement action for at least some platforms expected around **mid-2026**, subject to evidence.
- These platforms are the focus of eSafety's investigations because they have the largest numbers of child users and present higher risks of harm.
- Investigations involve gathering evidence to assess whether the steps taken by platforms are reasonable, and validating the information received from platforms.

Contact: s 22
Phone:

Cleared by: s 22, Executive Manager, ICE
Date: 15/04/2026

- eSafety is continuing to collect and assess evidence to determine whether platforms have failed to implement appropriate systems and processes, rather than focusing solely on the presence of individual under-16 accounts.
- Early research and community feedback indicate a **reduction in under-16 account ownership** following commencement of the SMMA obligation (from 49.7% to 31.3%); however, a significant proportion of children continue to **retain or regain accounts**.
- eSafety continues to monitor potential migratory patterns of social media use by children under the age of 16 and will adjust its regulatory focus as needed to ensure age-restricted social media platforms operating in Australia are complying with their obligations.

Background

Accounts removed and access prevented

- As at mid-December 2025, platforms reported the removal, deactivation or restriction of approximately **4.7 million** age-restricted accounts, based on information provided to eSafety through compulsory information-gathering notices.
- By March 2026, more than **300,000 additional accounts** were prevented from signing in and accessing age-restricted social media platforms.
- This new figure includes both **accounts that existed pre-10 December 2025**, that may not have been identified initially by platforms for a range of reasons including that they had a declared age of over 16 years, but also **new accounts** created and attempted to be created by users under 16 years since 10 December 2025.
- While this is a positive step, the number of accounts removed on its own is not determinative of compliance with the obligation to take reasonable steps, as detection and deactivation of accounts is only one of several ongoing measures platforms are required to implement.
- eSafety has made a public interest immunity claim (**Attachment A**) over the disaggregated platform numbers and information obtained by eSafety under its 11 December 2025 compulsory notices more broadly.
- The PII claim has been made on the basis that disclosure would or might reasonably be expected to prejudice eSafety's investigations into providers' compliance with the SMMA obligation.

Regulatory concerns about platform practices

- eSafety has identified a range of **poor or ineffective practices**, including:
    - Messaging that **encourages children aged under 16 to attempt age assurance** even where their declared age prior to 10 December was under 16 years of age.
    - Allowing **repeated attempts at the same age-assurance method**, even where there are signals that it might be providing a false result.
    - Inaccessible or **ineffective mechanisms for reporting children** aged under 16.
    - **Insufficient systems** to stop children aged under 16 from **creating accounts**.
- These practices raise concerns about whether some platforms have taken **reasonable steps** to comply with the SMMA obligation.
- An assessment of reasonable steps is context-dependent and holistic, requiring consideration of all measures implemented by a platform, rather than any single control.
- eSafety's regulatory guidance sets out our expectations regarding reasonable steps, including that platforms should take a **layered or 'waterfall' approach** across the user journey, combining measures to build cumulative confidence in a user's age.
- eSafety has communicated both our expectations and our concerns to platforms directly.

Improvements in practice

- Our engagements with platforms have led to some improvements being implemented. We have observed (including through user-testing) that:
    - The age ratings of Snapchat, Facebook and Instagram have been updated from 13+ to 16+ on the Australian Apple App Store.
    - Snap, Meta and TikTok have improved their underage user reporting pathways, including through increased discoverability and updates to language and Help pages.
    - Google has introduced new age verification requirements when some users attempt to change their date of birth.
- Whilst it is positive to see these improvements, eSafety is still assessing whether the steps taken by platforms at particular points in time were reasonable as well as whether the steps now being implemented are reasonable in their totality. Importantly, what might have been reasonable at the 1, 2, and 3 month marks might not be reasonable at the 6 month or even 12 month mark. That is why continuous improvement is expected, but also just because a platform has now taken certain steps doesn't mean they shouldn't have done so earlier.

Investigations and enforcement activity

- eSafety has issued 27 information-gathering notices to 10 platforms to investigate and assess their compliance with the SMMA obligation.
- eSafety is currently investigating potential non-compliance by **Snapchat, TikTok, Facebook, Instagram and YouTube**, with decisions about any enforcement action expected for at least some platforms by mid-2026, subject to evidence.
- Investigations focus on whether platforms have implemented appropriate **systems and processes**, not merely whether some under-16 users remain on services.
- Where eSafety considers a provider of a platform has not taken reasonable steps, we have a range of **enforcement options** available, including:
    - giving and publishing a platform provider notification
    - seeking a court enforceable undertaking from the platform provider
    - issuing an infringement notice
    - seeking court-ordered injunctions or civil penalties of up to $49.5 million.
- eSafety considers insights from a range of sources, including **submissions** from members of the public, and continues to validate information through **testing, research, stakeholder engagemen**t and further information-gathering notices where required, while balancing transparency with the need to protect investigation integrity.

Legislative updates and platform assessments

- On 25 March 2026, the Minister for Communications registered a new legislative rule **to better target the law towards platforms with addictive or harmful design features**.
- In addition to the existing conditions set out in the Online Safety Act, the new legislative rule provides that platforms must also have one or both of the following conditions to be an age-restricted social media platform:
    - A **recommender feature**, that selects and displays material to end-users based on that end-user's information
    - A **logged-in feature**, defined as **endless-feed, feedback, or time-limited features**.
- eSafety has re-assessed platforms and confirmed they continue to meet the conditions for age-restricted social media platforms, including these new conditions. eSafety has also written to relevant platforms to confirm this position.

- The list of age-restricted social media platforms published on eSafety's website is not exhaustive. eSafety continues to engage with a range of services regarding their potential status as age-restricted social media platforms. The most current information regarding services that have self-assessed as in-scope is available on eSafety's website.

Early impacts and community feedback

- eSafety's parent pulse research indicates a reduction in social media account ownership among 8-15 year olds, from **49.7% prior to commencement to 31.3% after implementation**, suggesting early impact.
- However, survey results show that around **7 in 10 children** who previously held accounts on some major platforms continue to retain them.
- Within the first three months since the SMMA obligation took effect, eSafety received more than **960 submissions or enquiries**, primarily raising concerns about:
    - Children aged under 16 retaining or regaining accounts on platforms; and
    - Perceived inaction from platforms following reports of age-restricted accounts.
- Stakeholder engagement, including with **educators** has found mixed early experiences, with some children aged under 16 appearing to be relieved they are no longer on social media, and others seemingly celebrating their circumvention and retention of accounts.

Difficult questions

Where is the evidence that eSafety has moved from monitoring to enforcement?

- eSafety has communicated that we are currently investigating Facebook, Instagram, Snapchat, TikTok and YouTube, with decisions on possible enforcement action expected by mid-2026, subject to the evidence.
- eSafety has used and continues to use information-gathering powers to obtain information relevant to assessing and investigating platforms' compliance.
- As explained in eSafety's SMMA compliance update published on 31 March 2026, we are validating information through testing, research, stakeholder engagement and further information-gathering notices where required, while balancing transparency with the need to protect investigation integrity.

Will eSafety be updating its Social Media Minimum Age Regulatory Guidance for industry?

- eSafety has publicly committed to reviewing the regulatory guidance by mid-2026.
- Given the current guidance was based on significant consultation conducted under a year ago, the review is unlikely to introduce significant changes.
- To support the review, eSafety has sought targeted feedback from age-restricted social media platforms and age assurance experts. Any feedback will focus on potential minor updates or clarifications, such as useful examples, while ensuring regulatory certainty and avoiding any outcome that could prejudice current or future enforcement action.

What does "reasonable steps" mean in practice?

- Enforcement action requires sufficient evidence that the platform has not taken reasonable steps to prevent children aged under 16 from having accounts.
- Whether a platform has taken reasonable steps is contextually dependent and requires a review of both the regulatory landscape and a business's circumstances. It is not a prescriptive test with a one-size-fits-all approach but instead requires a review of all steps taken in totality.
- Ultimately, if enforcement proceeds to court, the question of what constitutes reasonable steps and whether they have been taken is determined by the court on the evidence and context.

Is there any evidence the SMMA is having a positive impact?

- Early research and feedback indicate a reduction in social media account ownership among children under 16. eSafety's parent pulse survey found that almost half (49.7%) of surveyed parents reported their child had their own account on at least one platform prior to the restrictions coming into effect. This proportion decreased to 31.3% following the SMMA.
- Educators have also reported some early positive signals, including students expressing relief at no longer being on social media.
- eSafety has commenced a longer-term evaluation to assess impacts over time.

If asked about the High Court challenge

- Reddit is exercising its democratic right to challenge these laws.
- We will continue to implement this legislation and assess compliance.
- Notwithstanding the legal challenge, Reddit is engaging with eSafety cooperatively.

Attachment

A: Correspondence from eSafety Commissioner to Minister Wells re: QoN PII claim

Australian Government | eSafetyCommissioner

19 March 2026

Attachment A

Hon. Anika Wells MP
PO Box 6022
Parliament House
Canberra ACT 2600
Sent by email: s 47F [redacted]@mo.communications.gov.au

Dear Minister Wells

Public Interest Immunity claim regarding information subject to Questions on Notice

1. I am writing to you regarding Questions on Notice (**QoNs**)[1] that relate to the social media minimum age ([2]) obligation and information that was obtained by eSafety under compulsory notices.
2. The QoNs refer to the 4.7 million accounts that were removed, deactivated or restricted by providers to comply with the SMMA obligation as at 10-12 December 2025 and specifically seek a breakdown of that number by platform (**disaggregated platform numbers**).
3. Before responding to the QoNs, eSafety has considered whether a public interest immunity (**PII**) claim should be made over the disaggregated platform numbers and information that was obtained by eSafety under its 11 December 2025 compulsory notices more broadly.
4. We recommend that a PII claim be made over this information, including the disaggregated platform numbers, on the basis that disclosure would or might reasonably be expected to prejudice eSafety's investigations into providers' compliance with the SMMA obligation. s 47G [redacted]

Grounds for PII claim

Disclosure would or might reasonably be expected to prejudice eSafety's law enforcement investigations

[1] SQ26-000121, SQ26-000150, SQ26-000151, see **Annex A**.

[2] Section 63D of the *Online Safety Act 2021* (Cth): A provider of an age-restricted social media platform must take reasonable steps to prevent age-restricted users having accounts with the age-restricted social media platform.

5. eSafety is not a law enforcement agency, such as a state or territory police force or service. However, eSafety can be considered a law enforcement agency when it is investigating and enforcing compliance with the *Online Safety Act 2021* (Cth) (**OSA**).

6. eSafety gave providers of key platforms compulsory notices on 11 December 2025 requiring information relevant to their compliance with the SMMA obligation as at 10 December 2025 (when the SMMA obligation came into effect).

7. In response to questions during the Additional Estimates hearing of the Senate Environment and Communications Legislation Committee on 10 February 2026, eSafety flagged that the information might be subject to a PII claim due to the potential prejudice to eSafety's investigations.

8. In our view, it would not be in the public interest to disclose information obtained by eSafety under its 11 December 2025 compulsory notices as there is a high likelihood that disclosure would or might reasonably be expected to prejudice eSafety's investigations for the following reasons.

9. Information provided under these compulsory notices forms part of eSafety's ongoing investigations into providers' compliance with the SMMA obligation. Because these investigations precede and inform decisions about whether enforcement action should be taken, such as civil penalty proceedings, the confidentiality of compulsorily obtained information is essential at every stage. If providers of age-restricted social media platforms become aware of the precise scope or direction of eSafety's investigations through disclosed information, they would have an obvious opportunity to shape their own responses to compulsory notices, including aligning their responses with those of other providers, or to take steps to remedy or conceal certain conduct or to comply creatively with the SMMA obligation before eSafety can take action.

10. More broadly, failure to maintain the confidentiality of information provided to eSafety pursuant to compulsory notices may also have a chilling effect on compliance with eSafety's compulsory information powers both under Part 4A and other parts of the OSA, thereby significantly limiting eSafety's ability to effectively investigate allegations of serious breaches. Already a provider has voiced reservations in providing similar data to that previously provided on the basis that eSafety may be required to disclose that data. Confidentiality obligations therefore protect not just the integrity of eSafety's investigations, but importantly the credibility and effectiveness of not only the social media minimum age obligations but also the entire OSA and the protections that offers the Australian public.

11. It is accepted, however, that the confidentiality of compulsorily obtained information is not absolute. Where investigations have concluded, the justification for maintaining confidentiality over that information may fall away. Once those investigations have concluded or have sufficiently progressed such that disclosure no longer risks prejudicing the outcome, we accept that information obtained under the 11 December 2025 compulsory notices may be more suitable for disclosure at that time. This would of course require a case-by-case assessment.

12. We consider that the disclosure of information obtained by eSafety under its 11 December 2025 notices, including the disaggregated platform numbers, would or might reasonably be expected to prejudice eSafety's ongoing investigations into providers' compliance with the SMMA obligation. On this basis, we recommend that a PII claim be made over this information.

s 47G

[redacted]

Yours sincerely

Julie Inman Grant
eSafety Commissioner

Annex A: Questions on Notice

Departmental Question Number: SQ26-000121

Senator Dean Smith asked:

Senator DEAN SMITH: What we are seeking to do is to make sure that the numbers that you have provided, that are now in the public domain, that are being used by the head of government, and the minister, are, in fact, accurate. This is a scrutiny process.

Ms Inman Grant: Sure.

Ms Snell: I want to first just talk to the committee a little bit about how we got those numbers to give you some confidence in the overall figure. Firstly, as the commissioner has referred to, we issued information notices to in relation to 10 platforms. I can confirm those platforms were Snap, Reddit, YouTube, X, Twitch, Kick, Threads, Instagram, Facebook and TikTok. We required them to give us figures as of particular dates. The first one was we required them to give us figures by 18 December relating to, specifically, the immediate few days on and around 10th December. The figures were very much a point in time at that point in time. Those were required under compulsory information notices. That means that there's an obligation for them to respond, and there are penalties if they fail to respond or if they provide false information. On that basis, we believe there's a reasonable ability to have confidence in the numbers that we received. What's also important to understand is that those notices were issued as part of regulatory investigations that are ongoing, and it is important that we maintain the protection of those investigations in the sense that we don't want to compromise those. As we continue to investigate, should we become aware that the information that they provided was false or misleading, or should we have other concerns around whether they have taken reasonable steps, and we wish to take that to court or use other enforcement powers, we do not want to give them any ability to question or undermine our investigative processes. That said, what I can say is that we can take on notice the extent to which we can share specific information that we might have received under those investigation notices. I don't have the numbers of each individual platform before me here today to give to you right now.

Senator DEAN SMITH: Really?

Ms Snell: Really. I don't. I can tell you the 4.7—

Senator DEAN SMITH: Sorry, can I interrupt?

Ms Snell: Certainly.

Senator DEAN SMITH: 4.7 million is a number that has been bandied around in the public domain, and you wouldn't have thought to bring, in your estimates file, a detailed breakdown of those 10 platforms in terms of how you would get to 4.7 million?

Ms Snell: I think it's possible that it's appropriate for us to make a PII claim in respect of that. That's something we would like to explore further. I'm not saying, no, we can't give it to you, but I am saying that there is a process that we think we need to go through. [...]

Senator DEAN SMITH: Have you provided advice to anyone in government? That's the department, the minister or the Prime Minister's office in regard to the disaggregated 4.7 million deactivated, removed and restricted accounts?

Ms Snell: No, we have not.

Senator DEAN SMITH: But you have been requested that disaggregated number by the department of communications because that was their evidence to this committee earlier today. You have had it requested, but you've not provided it.

Ms Snell: I'm not aware of a specific request. We've had discussions with them, again, about the issue of the fact that we've received that information under compulsory information notices and that we consider that information to therefore be subject, potentially, to a PII. We're not disclosing that beyond eSafety in terms of our investigation processes.

Senator DEAN SMITH: They understand that, if they were to ask for it formally, you would say that you're not legally empowered to give them that figure?

Ms Snell: We consider it as not appropriate to disclose that information at this point in time, whilst the investigations are on foot. There may come a point in time, and it may be that if we take this question, the question of the individual numbers, on notice that we will have further consideration as to whether that's likely to prejudice the investigations or not.

Departmental Question Number: SQ26-000150

Senator Fatima Payman asked:

1. In an SMH article that the eSafety Commissioner was interviewed for, it was reported that, on 11 December, she was going to "issue information notices to every major platform demanding baseline data: how many under-16 accounts existed, how many were deactivated, what technologies were deployed." To which services were these information notices sent to?

2. From which services has eSafety received a response?

3. For each age-restricted social media platform, how many under-16 accounts have these services reported as having on their platforms?

4. Have any of the age assurance technologies used by these services been found not to meet the "reasonable steps" requirement? If so, which technologies and how did eSafety reach that conclusion?

Departmental Question Number: SQ26-000151

Senator Fatima Payman asked:

The Prime Minister has said that the ban has 'exceeded our expectations'. In December, no one at the table was willing to be drawn on Senator Smith's question on this matter, which was taken on notice, but does the government have any metrics that it is using to gauge the efficacy of the ban?

ESAFETY'S REVIEW OF 'INFORMAL NOTICES' OR COMPLAINT ALERTS POST-BAUMGARTEN

Key Points

- The February 2025 decision in *Baumgarten*[1] was relatively confined to the unique **process facts** following the complaint.
- eSafety updated its **processes** (**Attachment 2**) after the ART decision to further emphasise that the contact from eSafety is to:
    1. alert the recipient to the complaint
    2. emphasise that no action is required.
- eSafety has undertaken a review of previous complaints given in 2023/24 and 2024/25 which contain similar features to the complaint in Baumgarten (**Attachment 1**).
- End users are generally advised by platforms where platforms remove their posts. They are always advised when eSafety causes material to be removed. That enables them to take steps in response.
- eSafety has not had received any contact from any other end users that would suggest any similar circumstances exist.

The distinguishing features

- The complaint about the post in this matter had three key distinguishing features:
    1. Submission to a legal portal that was separate from communication sent via email or general enquiries portal,
    2. There was a reference to a section of law as a source of authority for the alert (as this was required in the portal), and
    3. Action was taken with respect to the material (i.e. material the subject of the alert was removed).

[1] Baumgarten and eSafety Commissioner (Guidance and Appeals Panel) [2025] ARTA 153 (26 February 2025) and eSafety Commissioner v Baumgarten [2026] FCAFC 12 (18 February 2026)

Background

eSafety's review of 'Informal notices' or complaint alerts post-Baumgarten

The Full Court and ART decisions

- In the Baumgarten matter, the Full Federal Court upheld a decision of the Administrative Review Tribunal (ART) which found that an informal complaint alert given to X Corp. by eSafety which asked X Corp. to consider whether a post made by Ms Baumgarten contravened X Corp.'s terms of service was a legally reviewable decision by the ART.

Facts of the Baumgarten matter

- eSafety assessed a complaint that we considered did not meet the threshold for Adult Cyber Abuse, but may have breached X's terms of service.
- eSafety communicated to X via their portal a request asking them to review a post against their terms of service. X removed the post. X advised the end user who made the post that they had withheld the post in Australia.
- eSafety made similar contact with Instagram about a potential breach of their terms of service. Meta did not remove the content. eSafety took no further steps.

Historic processes relevant to the Baumgarten matter

- Historically, many platforms preferred that eSafety flag content informally and also preferred us to do so via platform portals as opposed to email
- However, we are observing a shift to more providers not taking steps to address content on their services unless they receive a formal notice

4 updates to our processes since Baumgarten Tribunal decision in February 2025

1. Greater use of service provider notifications - (SPNs) to bring material to a platform's attention where legislative requirements to give an SPN are met.
2. 'Complaint notifications' rather than 'informal requests' - where we do contact platforms with a voluntary request, we provide complaint notifications in place of 'informal requests' that clearly specify that there is no legal obligation or requirement for action and that the correspondence is not a legal notice. We emphasise that it is at the platform's discretion as to what further action they take, if any.
3. Updated complaint notification template emphasising that it is a **notification**, and no action is required - eSafety updated its template for what used to be

called ‘complaint alerts’ to make these clarifications. eSafety’s current complaint notification template is at Attachment 1. Please note that this template is used for adult cyber abuse, child cyber-bullying and image-based abuse complaint schemes.

4. Confirmed contact details with platforms for different correspondence - eSafety has reached out to providers to re-confirm their preferred avenues for different types of eSafety correspondence, including statutory notices and voluntary complaint notifications.

What we have done to review historic communications (though we have no legal obligation to do so)

- The judgment was relatively confined to the facts of the particular notification and, in any event, the judgment should not be applied retrospectively.
- There is no legal obligation on eSafety to take action with respect to any complaint notifications or even to review alerts given prior to the conclusion of the Baumgarten proceedings.
- eSafety has undertaken a review of complaint alerts sent to X and Meta (Facebook and Instagram) for the Adult Cyber-Abuse, Child Cyberbullying and Image Based Abuse schemes in FY 2023/24 and 2025/26 with what we believe to be the key distinguishing features of the Baumgarten complaint as parameters for our review, namely:
    1. Submission to a legal portal separate from communication sent via email or general enquiries portal;
    2. Reference to a section of law as a source of authority for the alert; and
    3. Action was taken with respect to the material (i.e. material the subject of the alert was removed)

Data Summary

Based on the data below:

- A total of 1,214 alerts were sent to Meta and 78 alerts were sent to X across all schemes for 2023/24 and 2024/25
- For the ACA and CB schemes, the majority of these alerts to X were sent via email whereas the majority of the alerts to Meta were sent via Meta’s official requests portal
- 81% of complaint alerts sent by eSafety to Meta had all or some of the material removed across all 3 schemes
- 66% of complaint alerts sent by eSafety to X had all or some of the material removed across all 3 schemes

Attachment 1

The total number of complaint alerts eSafety sent to X and Meta in FY 2023/24 and 2024/25

Meta – Total of 1,214 alerts across all schemes for 2023/24 and 2024/25

- IBA: 282 in 2023/24; 112 in 2024/25
- ACA: 199 in 2023/24; 107 in 2024/25
- CB: 277 in 2023/24; 237 in 2024/25

X Corp – Total of 78 alerts to X across all schemes for 2023/24 and 2024/25

- IBA: 20 in 2023/24; 23 in 2024/25
- ACA: 23 in 2023/24; 7 in 2024/25
- CB: 5 in 2023/24; 0 in 2024/25

The number of complaint alerts with the same 3 features that eSafety sent to X and Meta in FY 2023/24 and 2024/25

1. **Legal requests portal**

The Number of complaint alerts which were sent via **X's** legal requests portal or a similar legal portal at **Meta** across all schemes

- Alerts to **Meta**: 892 of 1,214 alerts sent via provider online form or webform
- Alerts to **X**: 47 of 78 alerts sent via provider online form or webform

By scheme

- For the ACA and CB schemes, 61% of alerts to **Meta** were made to Meta's 'official requests' form and 39% were sent via email
- For the CB scheme, 100% of alerts to **X** were sent via email
- For the ACA scheme, 27% of alerts to **X** were made to X's legal requests form and 73% were sent via email

2. **Referred to a section of the Online Safety Act (sampling exercise)**

Number of complaint alerts sent via a portal which referred to a section of the Online Safety Act in the mandatory field requiring a source of law

- Based on a review of a sample of alerts to **Meta** over 2023/24 and 2024/25, none of the alerts referred to a section of the Online Safety Act. One of these

alerts specifically stated 'This is *not* a removal notice under the Online Safety Act'.

- Based on a review of a sample of alerts to **X** over 2023/24 and 2024/25, 2 alerts referred to a section of the Online Safety Act.

3. Platforms took action (all complaints, not sampling)

Action taken by X and/or Meta (if any) in response to the complaint alert

- Alerts to Meta: For 176 of 1,214 total alerts to Meta, none of the material was removed

- 81% of complaint alerts sent by eSafety to Meta had all or some of the material removed across all 3 schemes. 14% was not removed at all.

- In 2% of cases, other action was taken, which may include removal notices being given after complaint alerts did not lead to the material being taken down. In the remaining 3% of cases, there is insufficient data to determine what occurred.

- Alerts to X: For 20 of 47 total alerts to X sent via X's legal request webform, none of the material was removed

- 66% of complaint alerts sent by eSafety to X had all or some of the material removed across all 3 schemes. 26% was not removed at all.

- In 4% of cases, other action was taken, which may include removal notices being given after complaint alerts did not lead to the material being taken down. In the remaining 4% of cases, there is insufficient data to determine what occurred.

Data

Data available at: DDIR-521 - Complaint alerts sent to X and Meta 01.07.2023 to 30.06.2025.xlsx

Attachment 2

eSafety's current complaint notification template for social media services, designated internet services and relevant electronic services

Dear [Platform]

The eSafety Commissioner is responsible for improving and promoting online safety for Australians and administering a complaints system for certain types of harmful online material.

For more information about eSafety's role and functions, please refer to our website and the *Online Safety Act 2021* (Cth) (the **Act**).

Why we are writing to you

eSafety has received a complaint about material that appears to be provided on your service. The complaint is about material located at the following URL(s) (the **Material**):

- [URL]
- [URL]
- [URL]

In summary, the complaint [brief narrative of the complaint].

This letter/email is notifying you that the Material may be in breach of your [terms of service/rules/policies/standards etc.].

Voluntary Request

eSafety is requesting that you review the Material against your [terms of service/rules/policies/standards etc.] and take any action/s you consider appropriate.

We are also requesting that you confirm receipt of this correspondence and that you inform us as soon as is reasonably practicable of what action, if any, you have taken. We appreciate your assistance in this matter.

Please note: eSafety is ***not requiring*** any action from you under the Act – any action you take is voluntary.

If you need further information, or have any questions or concerns, please feel free to contact us at email address [insert].

2026 - 2027 Budget Estimates

Environment and Communications

Lead/Support contact: Sarah Vandenbroek / Anthea Fell

SB26-000064

SUBJECT: Online Safety: Industry Codes and Standards

Key Deliverables

- Under the *Online Safety Act 2021* (the Act), industry has developed 2 sets of codes to protect Australians from harmful content online:
  - the Unlawful Material Codes, which protect Australians from the most seriously harmful online content, such as child sexual exploitation material and pro-terror material;
  - the Age-Restricted Material Codes, which protect young Australians from seeing certain content, including porn, suicide and self-harm material. Age assurance measures are required under some parts of these codes.
- These codes have been registered by the eSafety Commissioner, who is responsible for enforcement.
- The Australian Government has also increased the penalties for breach of industry codes and standards to up $49.5 million for bodies corporate.

Talking Points

- The *Online Safety Act* requires industry to develop codes to keep Australians safer online.
- The latest set of codes developed under the Act – the Age-Restricted Material codes – will help protect children from exposure to age-restricted content across a range of internet services.
- This is the second set of codes to come into effect, with the Unlawful Material Codes having been in effect since December 2024.
- The risks young Australians face are real. Research from the eSafety Commissioner reveals that 1 in 3 young people who had seen online pornography first encountered it unintentionally before the age of 13.
- Any service that hosts or facilitates access to age-restricted content (like pornography, very violent or self-harm material) needs to ensure measures are in place to limit under 18s from accessing that content – including age assurance.
- The codes include practices that some companies are already using, such as safe search functions that blur sensitive content.
  - Age assurance will not be required to use search engines like Google if you are not logged in.
  - You only need to prove your age if you want to access age restricted material.

- The codes require industry to better protect children from harms that come about from AI intended for adults, such as sexualised chatbots.
- Privacy protections have been built into all aspects of Australia's online safety policy. Under the codes, services must comply with Australia's privacy laws.
- Specific questions about the operation of the codes are best answered by eSafety.

Key Issues

- The industry codes were developed in 2 phases: the first focused on the most seriously harmful content (the Unlawful Material Codes), and the second focused on age-restricted content (the Age-Restricted Material Codes).
- eSafety is responsible for enforcing the codes.
  - eSafety will take enforcement action where a service demonstrates systemic non-compliance.
  - Non-compliance can result in penalties of up to $49.5 million.

Unlawful Material Codes and Standards

- The first phase of codes and standards covered illegal material that would be Refused Classification under the National Classification Scheme.
- It includes the most seriously harmful online material such as child sexual exploitation material, pro-terror material and extreme crime and violence content.
- The eSafety Commissioner registered 6 industry codes covering social media services, app distribution services, hosting services, internet carriage services, equipment services and search engine services.
- The Commissioner also made 2 standards covering relevant electronic services, and designated internet services.

Age-Restricted Material Codes

- The Age-Restricted Material codes are now in place.
  - The dates these codes entered into force is at **Attachment A**.
- The purpose of the codes is to prevent children inadvertently accessing adult material like pornography, very violent or suicide/self-harm material.
- The codes also uplift the overall safety standards of online services.
- While content like porn is not illegal, it is regulated. These codes reflect laws which exist offline.
- Age assurance technology will be used in parts of these codes.

Impact of the codes on using the internet

- The Age-Restricted Material codes require industry to use age assurance, and other tools to limit children's inadvertent access to age-restricted material.
- People only need to prove their age to view adult material.
- Search engines will continue to be available, and age assurance is not needed to use them in a logged-out state.
- The codes require platforms to make a broader uplift in safety.
  - For example, if someone searches for suicide or self-harm material, any material promoting this will be downranked by the search engine, and health information and support services will be promoted.
  - The codes include practices that some companies are already using, such as safe search functions that blur sensitive content where they are not sure of a user's age.

Privacy protection under the codes

- Under the industry codes, services need to comply with Australia's privacy laws.
- The Office of the Australian Information Commissioner is the Australian privacy regulator. It can act whenever it considers an organisation is in breach of Australian privacy law.
- The Head Terms of the codes specify that services must consider whether age assurance measures comply with privacy laws and whether their impact on user privacy is proportionate.
- eSafety's regulatory advice is clear:
  - Government ID cannot be the only option to prove your age on any service.
  - eSafety does not expect service providers to retain personal information.
- *Note: Under the codes, it is acceptable to use government ID as one of a range of methods of age assurance.*

Use of Virtual Private Networks (VPNs)

- Under the codes, there are requirements that service providers must take reasonable steps to prevent workarounds like VPNs so eSafety will look at this when considering compliance with codes.
- This is similar to eSafety's regulatory guidance for the social media minimum age, where eSafety considers VPN detection as a reasonable step to prevent underage users from having an account.
- Through the Age Assurance Technology Trial, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts knows that tech companies can tell when a VPN is in use.

Background

- Under the Act, illegal and age-restricted online content is called Class 1 and Class 2 material and is defined by reference to Australia's National Classification Scheme.
- The codes and standards outline the steps that industry must take to prevent access, exposure, or distribution of, Class 1 and Class 2 material.
- The industry codes framework covers 8 sections of the online industry: social media services, relevant electronic services (RES), designated internet services (DIS), search engine services, hosting services, app distribution services, equipment services, and internet carriage services.
- Details of when the codes and standards entered into force is at **Attachment A.**

Supporting Information

Relevant Media Reporting

- 'Age verification for R-rated games and websites raises privacy concerns', Ahmed Yussef, ABC, 9 March 2026, www.abc.net.au/news/2026-03-09/privacy-concerns-about-age-verification-r-rated-games-websites/106432440.
- 'Major porn sites have blocked Australian users to protest new laws. Will kids be better off?' Giselle Woodley and Megan Lim, The Conversation, 10 March 2026, www.theconversation.com/major-porn-sites-have-blocked-australian-users-to-protest-new-laws-will-kids-be-better-off-277835

Attachments

- A: Entry into force of the Unlawful Material Codes and Standards and the Age-Restricted Material Codes.

Attachment A

Entry into force of the Unlawful Material Codes and Standards and Age-Restricted Material codes

Code	Relevant Dates	Notes
Unlawful Material Codes and Standards		
Social Media Services Code	16 December 2023 – came into effect	*Prevent access and exposure to the highest-harm online material, such as child sexual abuse material and pro-terror content.*
Internet Carriage Services Code		
App Distribution Services Code		
Hosting Services Code		
Equipment Services Code		
Search Engine Services Code	12 March 2024 – came into effect	
Designated Internet Services (DIS) Standard	22 December 2024 – came into effect	*Drafted by the eSafety Commissioner after judging that the draft codes for these services were not acceptable. The DIS Standard also covers 'nudify apps' that use generative AI to create pornography or 'nudify' images without effective controls to prevent the generation of material such as child exploitation and abuse content.*
Relevant Electronic Services Standard	22 December 2024 – came into effect	
Age-Restricted Material Codes		
Search Engine Services Code	27 December 2025 – all provisions (except age assurance provisions) came into effect	*Protect children from exposure to pornography, violent content, and themes of suicide, self-harm and disordered eating.*
	27 June 2026 – age assurance provisions come into effect	
Enterprise Hosting Services Code	27 December 2025 – came into effect	
Internet Carriage Services Code	27 December 2025 – came into effect	

Code	Relevant Dates	Notes
Relevant Electronic Services Code	9 March 2026 – came into effect 9 September 2026 – age assurance provisions come into effect for the APP distribution code	
DIS Code		
Social Media Services (Core features) Code, and Social Media Services (Messaging features) Code		
Equipment Services Code		
App Distribution Services Code (APP)		

GENERAL MANAGER - CORPORATE AND STRATEGY

ESTIMATES BACKGROUND – May 2026

1	Finance Numbers	1.1	2026-27 Budget Outcome
		1.2	Key Financial Statistics
		1.3	Travel Expenditure and Qantas/Virgin memberships
		1.4	Commissioner salary increase and hospitality
2	2024-25 Annual Report	2.1	2024-25 Financial Outcome
		2.2	Financial tables – summary of all tables in the Annual Report
		2.3	Appendix 1.12 – standard financial table
		2.4	Note 9 - disaggregation of eSafety balances
		2.5	Appendix 1.10 – Outcome table
		2.6	Media and Advertising expenditure
		2.7	Consultants expenditure
		2.8	Non-consultants expenditure
		2.9	Contractors expenditure
		2.10	Supplier Expenditure
		2.11	Operating Loss
		2.12	Non-financial component – Performance Measures
3	Budget	3.1	2026-27 PBS budget breakdown
		3.2	SMMA Funding
		3.3	Previous Financial Year results
		3.4	Funding background
		3.5	Internal Budget allocation
4	Finance other	4.1	s83 Breach
		4.2	Special Account
		4.3	Austender media questions
5	Staffing	5.1	Staffing
		5.2	Wellbeing and Strategic HR
6	Research & Eval	6.1	Evaluation of SMMA
		6.2	Evaluation protocol paper
		6.3	Q&A
7	Education, Engagement & Awareness	7.1	StratComms
		7.2	EPaC [incl Deepfakes, Vulnerable Communities and SIA cost/MOU]
		7.2	Grants
8	Gov & Business Ops	8.1	General Enquiries
		8.2	TFA Service
		8.3	OSA Review
		8.4	eSafety's submissions to inquiries
		8.5	Age Assurance
9	Media Releases	9.1	Media Releases

2026-27 Budget Outcome

The **2026-27 Budget** includes the following impacts:

1. **Technology Facilitated Abuse Support Service**
   Funding of $5.434m for 2026-27
   One year extension of the Technology-Facilitated Abuse Support Service to assist frontline workers and victim-survivors to navigate and respond to tech-facilitated abuse

   This is part of the following package:
   Ending Gender-Based Violence – continued investment
   The Government will provide $308.6 million over five years from 2025–26 (and $15.9 million per year ongoing) to further support women and children leaving violent relationships and strengthen the frontline family, domestic and sexual violence workforce.
   From Budget Paper No.2 Budget Paper No. 2 | Budget 2026–27

2. **National Strategy to Prevent and Respond to Child Sexual Abuse**
   Funding of $0.656m for 2026-27
   One year extension of this program that focuses on safeguarding children and young people from online harm, including sexual abuse and exploitation through resources, guidance and training.

3. **Government Response to the Antisemitic Bondi Attack**

   As per the ACMA PBS:
   Funding: Not for publication

	Program	2025-26 $'000	2026-27 $'000	2027-28 $'000	2028-29 $'000	2029-30 $'000
Payment measures						
Government Response to the Antisemitic Bondi Attack Departmental payment	1.3	nfp	nfp	nfp	nfp	nfp

From Budget Paper No.2 Budget Paper No. 2 | Budget 2026–27

Government Response to the Antisemitic Bondi Attack
Part of a broader package "Government Response to the Antisemitic Bondi Terrorist Attack" - $207.4 million over five years from 2025-26 (and $8.1 million ongoing) to combat the influences of antisemitism, violent extremism and hate in Australian communities, and respond to the recommendations of the Special Envoy's Plan to Combat Antisemitism.

The Government committed to support eSafety in providing online safety advice to address antisemitism following the Bondi terrorist attack.

$1.0 million in 2025–26 was prioritised from eSafety's existing resources to strengthen engagement and provide advice and support to the Government, the Department and the Special Envoy to Combat Antisemitism to enhance regulatory responses to online hate and progress duty of care reforms under the Online Safety Act.

Continued on next page

Government Response to the Antisemitic Bondi Attack (cont)

Resource efforts have also focussed on:

- analysis and responding to online hate complaints,
- strengthening partnerships and sharing intelligence with federal, state and territory law enforcement agencies facilitating the rapid referral of harmful material,
- ongoing review of online abuse support materials,
- sharing regulatory insights and advice to better address online hate (eg work with Standing Council of Attorneys General), and
- responding to requests from the Royal Commission on Antisemitism and Social Cohesion.

4. **Further Reducing Spending on Consultants, Contractors and Labour Hire, and Non-wage Expenses - one year extension**

   Funding reduction of $1.871m

   One year extension, in 2029-30, of the 2025-26 Budget measure *'Savings from External Labour – extension'*. The whole of Government will achieve further savings by reducing spending on external labour.

From the Women's Budget Statement 2026-27

Women's Budget Statement | Budget 2026–27

Gender analysis in practice: Technology-facilitated gender-based violence

Technology can be used to perpetrate FDSV, including coercive control, cyberstalking and deepfake images and videos. The Government is committed to protecting women and children online through a number of reforms.

Since 9 March 2026, the Age-Restricted Material Codes limit Australians under the age of 18 from accessing adult material, including pornography. Evidence shows that the viewing of harmful content can be a driver towards FDSV through shaping negative attitudes towards gender, promoting harmful sexual behaviours and increasing misogynistic views.

The Government has enacted reforms to address technology-facilitated abuse that disproportionately impacts women. The *Privacy and Other Legislation Amendments Act 2024* outlaws the malicious release of personal data online, or 'doxxing'. The *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* strengthens existing offences and creates new offences prohibiting the creation and nonconsensual sharing of sexual material online, including material created or altered using technology (sexual deepfakes).

Further reforms will support action against technology-facilitated abuse. The Government has committed to legislating a digital duty of care, which will place the responsibility on digital platforms to take reasonable steps to prevent foreseeable online harms and perform due diligence to make their platforms safer. It will focus on restricting access to content that is illegal or harmful to young people, as well as minimise the risk of harm from features such as artificial intelligence and algorithms.

Under a duty of care framework, platforms will be obligated to put in place systems and processes that prevent their services being used to cause harm. Additionally, there will be new bespoke powers introduced enabling the eSafety Commissioner to issue notices to remove nudify apps and websites.

Key Finance Statistics

Budget as per the 2026-27 PBS		2025-26	2026-27	Variance
	Departmental	$68.551m	$66.467m	-$2.084m
	Administered	$1.750m	$3.500m	$1.750m
	Total	**$70.301m**	**$69.967m**	**-$0.334m**

SMAA funding Received	2024-25	2025-26	2026-27	2027-28
• **$45.651m** over **four years**. **$12.3m** per year ongoing funding from 2028-29.				
40 ongoing ASL	$3.810m	$16.163m	$13.260m	$12.418m

SMAA evaluation contract amount	2025-26 GST inclusive	2026-27 GST inclusive	2027-28 GST inclusive	Total GST inclusive
	$765,791	$651,442	$163,105	**$1,580,338**

A recent QON asked:
Q: What is the expected cost of the two-year longitudinal survey as identified in the Statement of Work: Evaluation of the Social Media Age Restriction?
A: $1,460,839 GST inclusive
This answer did not include the delivery of a component funded by the Institute of Criminology. This amount is included in the table above.

Staffing numbers as at 30 April 2026			
	APS FTE	236	Under the Strategic Commissioning Framework, eSafety has converted approximately **27** positions from contractors to ASL [24-25 and 25-26]
	Contractors FTE	20	
	Total	**256**	

Travel expenditure		2024-25 Full year	2025-26 YTD to 30 April 2026
	Domestic travel	$0.670m	$0.446m
	Overseas travel	$0.349m	$0.152m
	Total	**$1.019m**	**$0.598m**

External Legal expenditure	2024-25 Full year	2025-26 YTD to 30 April 2026	
	$1.018m	$1.889m	2025-26 expense excludes costs paid to X Corp re Wakeley case of $0.624m.

Contractors and Consultants expenditure		2024-25 Full year	2025-26 YTD to 30 April 2026
	Contractor/Labour Hire	$12.114m	$5.652m
	Consultants	$2.182m	$1.184m
	Total	**$14.296m**	**$6.836m**

Employee expenses	31.354m

Contractors	5.65m
Consultants	1.184m
Suppliers	5.35m
Media & publishing	658k
Advertising & marketing	147K
Domestic travel	446k
International travel	152k
YTD expenditure	49.908m

Report Category	Natural Account	Natural Account	Contract Number	Description	Contract Value (inc GST)	YTD amount paid (exc GST)
Advertising and Marketing	Advertising	1281	ECOM00000040	Advertising services for subscriber campaign	$ 110,000	$97,175
Advertising and Marketing	Advertising	1281	ECOM00000111	Young people content and paid media	$ 110,000	$ 79,312
Advertising and Marketing	Advertising	1281	ECOM00000049	Paid search activity 2025/26	$ 88,000	$ 62,517
Advertising and Marketing	Advertising	1281	ECOM00000064	TFA + Kids traffic campaign	$ 66,000	$ 60,000
Advertising and Marketing	Advertising	1281	ECOM00000046	Advertising services for education resources	$ 49,500	$ 42,289
Advertising and Marketing	Advertising	1281	ECOM00000043	Coercive control awareness campaign	$ 22,000	$ 19,315
Advertising and Marketing	Advertising	1281	ECOM00000084	Be Connected NSW Seniors Card solus eDM and eNews	$ 16,500	$ 15,000
				Total	$ 462,000	$ 375,608
Media and Publishing	Marketing and Engagement	1288	ECOM00000038	Media buy for parents webinar campaign	$ 88,000	$ 57,550
Media and Publishing	Marketing and Engagement	1288	ECOM00000057	Brand Voice and Positioning Development	$ 53,339	$ 48,490
Media and Publishing	Marketing and Engagement	1288	ECOM00000077	Sextortion Campaign	$ 93,458	$ 44,962
Media and Publishing	Marketing and Engagement	1288	ECOM00000095	2026 Brand Tracker	$ 104,500	$ 33,250
Media and Publishing	Media Relations	1282	ECOM00000018	Social Media Management	$ 70,821	$ 24,553
Media and Publishing	Media Relations	1282	ECOM00000109	Social Media Management	$ 244,200	$ 74,000
Media and Publishing	Media Relations	1282	25CESC048	Campaign Monitor 2025-26	$ 69,960	$ 33,600
Media and Publishing	Media Relations	1282	25CESC026	Communications Support	$ 200,000	$ 35,160
Media and Publishing	Publishing and Printing	1285	ECOM00000051	Printing Early Years Resources	$ 28,391	$ 16,815
Media and Publishing	Publishing and Printing	1285	23CESC056	Provision of Warehouse Storage	$ 271,000	$ 82,802
Media and Publishing	Publishing and Printing	1285	ECOM00000062	Printing 'Let's Talk about Being Safe Online' Family Book	$ 19,604	$ 17,822
				Total	$ 1,243,274	$ 469,004
				TOTAL	$ 1,705,274	$ 844,612

Travel expenditure

	Domestic travel	Domestic travel	Overseas travel	Overseas travel

Travel expenditure All staff	2024-25 FY	2025-26 YTD To 30 April 2026	2024-25 FY	2025-26 YTD To 30 April 2026
	$0.670m	**$0.446m**	**$0.349m**	**$0.152m**

Travel expenditure Commissioner only	Domestic travel 2024-25 FY	Domestic travel 2025-26 YTD To 30 April 2026	Overseas travel 2024-25 FY	Overseas travel 2025-26 YTD To 30 April 2026
	$0.057m	**$0.046m**	**$0.103m**	**$0.020m**

Overseas travel expenditure All staff	**Funding Source**	**2017-18 to 2023-24 FY's**	**2024-25 FY**	**2025-26 FY To 30 April 2026**
	Funded by eSafety	$1.092m	$0.297m	$0.102m
	Funded by other agencies	$0.200m	$0.052m	$0.050m

The Commissioner has undertaken **22** overseas trips since her appointment in 2016. Trips undertaken since 2022-23:

Date	Location	Itinerary	Total
20-27 September 2025	USA	Speaking at the Stanford Trust & Safety Research Conference	$ 20,392.55
7-14 December 2024	USA	Global Online Safety Regulators network OECD events and Joint US and Australia Council on Combatting Online Child Exploitation	$ 28,825.58
9-22 November 2024	France	94th session of the OECD Digital Policy Committee	$ 37,255.42
15-26 September 2024	USA	Responsible Tech Summit	$ 36,689.85
13-27 January 2024	Switzerland, Belgium and Ireland	World Economic Forum, meetings with international policymakers and legislators	$ 26,402.58
6-11 October 2023	Japan	Internet Governance Forum	$ 13,399.04
8-28 September 2023	London, Germany, Italy and Singapore	Global Online Safety Regulators Network, Digital Policy Summit, Monash Gender and Family Violence Prevention Centre roundtable , Online Harms Symposium	$ 37,966.84
3-14 March 2023	USA	67th session of the UN Commission on the Status of Women	$ 19,844.40
13-22 January 2023	Switzerland	World Economic Forum	$ 25,338.53
12-24 November 2022	USA	Family Online Safety-Institute Conference	$ 35,270.80

Qantas / Virgin Lounge Memberships

AIRLINE	NAME	EXPIRY DATE	TOTAL
QANTAS	s 22	29/04/2027	
QANTAS		31/03/2027	
QANTAS		31/10/2026	
QANTAS		30/09/2026	
QANTAS		31/07/2026	
QANTAS		30/06/2026	
QANTAS		30/06/2026	
QANTAS		30/06/2026	8
VIRGIN		31/07/2026	
VIRGIN		31/07/2026	
VIRGIN		31/07/2026	3
QANTAS - Chairman's Lounge	JULIE INMAN GRANT		
Virgin - Beyond	JULIE INMAN GRANT		2
TOTAL			13

2026-27 PBS table breakdown	2025-26 Estimated actual $m	2026-27 Budget $m	2027-28 Forward estimate $m	2028-29 Forward estimate $m	2029-30 Forward estimate $m
Grants	2.500	2.500			
Grants - 2025-26 Movement of funds	-0.750	1.000			
Administered Total	**1.750**	**3.500**	**0.000**	**0.000**	**0.000**
Original base funding	10.309	10.309	10.309	10.309	10.309
Additional ongoing base funding Budget 2023-24	24.382	24.765	24.765	24.765	24.765
SMMA funding	13.163	13.260	12.418	12.283	12.283
Other impacts (including indexation)	0.809	1.165	1.774	2.159	2.810
Savings from External Labour - extension	-0.140	-0.129	-0.909	-0.566	
Savings from External labour, Advertising, Travel & Legal expenses	-1.022	-0.620			
Savings from 2025 Election Commitment	-0.908				
Savings from 2025-26 MYEFO		-1.990	-1.765	-1.469	
Saving from 2026-27 Budget		-0.105	-0.090	-0.086	-1.871
Total Base funding	**46.593**	**46.655**	**46.502**	**47.395**	**48.296**
NPP eSafety General awareness Initiative	0.100	0.100			
NPP Be Connected	4.034	4.082	4.134		
NPP National Strategy to Prevent Child Sexual Abuse	0.644	0.656			
NPP TFA Technical Support	5.600	5.434			
NPP Protecting Australians Online	1.633	1.653			
NPP Internal legal and Compliance	0.782				
Total NPP funding	**12.793**	**11.925**	**4.134**	**0.000**	**0.000**
Total Departmental Appropriation receipts	**59.386**	**58.580**	**50.636**	**47.395**	**48.296**
ACMA direct appropriation funding	8.909	8.909	8.909	8.909	8.909
Less ACMA capital funding	-1.821	-1.837	-1.837	-1.837	-1.837
Total ACMA funding	**7.088**	**7.072**	**7.072**	**7.072**	**7.072**
Expenses not requiring appropriation (depreciation)	**1.687**	**0.514**	**0.373**	**0.012**	
s74 External revenue	**0.390**	**0.300**			
Departmental Total	**68.551**	**66.467**	**58.081**	**54.479**	**55.368**
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**

Commissioner salary increase

Media article – January 20, 2026

How much senior bureaucrats are earning this financial year | The Canberra Times | Canberra, ACT

Australia's eSafety Commissioner Julie Inman Grant is taking home a $74,000 salary bump to enforce the government's social media ban this year, after senior agency heads collectively received pay increases of around 2.4 per cent.

The head of the national online safety regulator, who is leading the Albanese government's implementation of social media restrictions for under-16s, is earning an additional $73,790 in the 2025-26 financial year, bringing her annual salary to $533,550.

Senior public servants' and MPs' salaries and benefits are currently decided independently by the Remuneration Tribunal, which approved a 3.5 per cent pay rise in 2024.

Total remuneration is inclusive of salary, allowances, benefits and superannuation.

Response:

- The Remuneration Tribunal is responsible for independently setting the remuneration of the eSafety Commissioner. Remuneration details are publicly available on the Remuneration Tribunals website.
- On **16 April 2025**, the Remuneration Tribunal increased the remuneration of the eSafety Commissioner from **$459,760 to $521,040, an increase of $61,280**, in respect to additional functions under the Online Safety Act.
- A **further increase of 2.4%** was applied on 20 December 2025 to all Full-Time public office holders, increasing the eSafety Commissioners remuneration by **$12,510.**
- The two most recent increases total **$73,790.**
- Total remuneration is inclusive of salary, allowances, benefits and superannuation.

For comparative purposes:

eSafety Commissioner	**$533,550**
Chair, Australian Communications and Media Authority	$627,700
Deputy Chair, Australian Communications and Media Authority	$470,800
Aged Care Quality and Safety Commissioner	$533,550
Information Commissioner	$533,550
Australian Electoral Commissioner	$627,700
Chair, Australian Energy Regulator	$627,700
Chair/Chief Executive Officer, Clean Energy Regulator	$627,700
National Anti-Corruption Commissioner	$803,440
National Anti-Corruption Deputy Commissioner	$627,700
Chairperson, Australian Competition and Consumer Commission	$858,160

Commissioner Hospitality

Gifts and Benefits Register
Accepted
Period: Quarter 1
1 July 2025 to 30 September 2025

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality Gift / Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
24/07/2025	23/09/2025	Benefit	Commissioner	Communications Alliance	Complimentary ticket to attend the Communications Alliance 2025 Telecommunications Industry Excellence Awards	$290.00
25/08/2025	23/09/2025	Benefit	Commissioner	Queensland Police	Speaker invitation and complimentary ticket to the 2025 Youth, Technology and Virtual Communities Conference (YTVC) and dinner event.	$1,095.45
27/08/2025	5/09/2025	Hospitality	Commissioner	Sydney Morning Herald	Invitation to attend Press Gallery Mid-Winter Ball at Parliament House x 2 tickets.	$400.00
24/09/2025	16/10/2025	Benefit	Commissioner	Standford University	Invitation to speak and attend Trust and Safety Conference	$306.00

Declined
Period: Quarter 1
1 July 2025 to 30 September 2025

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality/Gift/ Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
26/8/25	23/9/25	Benefit	Commissioner	Minderoo Foundation	Invitation to attend as a contributor at the Minderoo AI Summit, an event convening leading global experts to identify and explore ways to improve stakeholder alignment and action towards safe and responsible AI.	Unknown

Gifts and Benefits Register
Accepted
Period: Quarter 2
1 October 2025 to 31 December 2025

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality/Gift/ Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
15/10/2025	22/12/2025	Gift	Commissioner	Nippon TV	Gift provided following interview with eSafety Commissioner (six pack of dried mangoes).	$110.42
20/11/2025	22/12/2025	Hospitality/Gift	Commissioner	Marie Claire	Complimentary ticket to attend the 2025 Women of the Year Awards and gift (Georg Jensen Cobra stainless steel pitcher).	$400.00
3/12/2025	22/12/2025	Benefit	Commissioner	Minister for Communications	Complimentary ticket to National Press Club Lunch - address by Minister Wells on Social Media Minimum Age bill.	$120.00

Declined
Period: Quarter 2
1 October 2025 to 31 December 2025

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality/Gift/ Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
5/12/25	22/12/25	Benefit	Commissioner	The Daniel Morcombe Foundation	Invitation to attend the 21st Annual Dance for Daniel in March 2026.	$285.00

Gifts and Benefits Register

Accepted
Period: Quarter 3
1 January 2026 to 31 March 2026

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality/Gift/ Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
18/02/2026	19/03/2026	Benefit	Commissioner	The Hatchery Co	Invitation to speak at the Women Unlimited Leadership Summit. Speakers were also provided tickets to the whole conference.	$4,299.00
1/03/2026	12/03/2026	Benefit	Commissioner	Qantas	Renewal of complimentary Qantas Chairman's Lounge membership to March 2027.	Unknown
8/03/2026	19/03/2026	Benefit	Commissioner	Australian Sports Commissioner	Invitation to attend the AFC Women's Asian Cup Australia 2026 - AUS vs KOR	$230.00

Declined
Period: Quarter 2
1 October 2025 to 31 December 2025

In the course of my duties as eSafety Commissioner, I received the following gifts and/or benefits whose value exceeds the stipulated threshold of $AUD100.00 (excluding GST).						
Date received	Date recorded	Itemisation of Hospitality/Gift/ Benefit	Received by (agency contact if not received directly by the agency head	Presented by (giver's name, organisation / country)	Occasion	Estimated value in $AUD
nil to report						

2024-25 Financial outcome

Expense type		24/25 actuals	*23/24 actuals*	Variance
Departmental	Operational expense	$55.751m	*$39.968m*	$15.783m
	Capital expense	$0.043m	*$0.730m*	(-$0.687m)
	Total	**$55.794m**	***$40.698m***	**$15.096m**
Administered	Grants provided	$1.979m	*$2.335m*	(-$0.356m)
	Be Connected expense	$0m	*$3.762m*	(-$3.762m)
	Total	**$1.979m**	***$6.097m***	**(-$4.118m)**
Total		**$57.773m**	***$46.795m***	**$10.978m**

The growth in overall expenditure is related to funding received for new programs, primarily SMMA and an uplift to eSafety's internal legal and compliance functions.

The Be Connected program moved from administered expenditure to departmental expenditure in 2024-25.

The YTD expenditure in Media and Marketing natural accounts includes services for:

- video services and production
- Graphic design
- Media relations
- Publishing and Printing
- Advertising
- Marketing and Engagement

Main YTD costs are in relation to advertising and relate to the following contracts:

Contract Number	Description	Contract Value (inc GST)	YTD amount paid (exc GST)
ECOM00000040	Advertising services for subscriber campaign	$ 110,000	$97,175
ECOM00000111	Young people content and paid media	$ 110,000	$ 79,312
ECOM00000049	Paid search activity 2025/26	$ 88,000	$ 62,517
ECOM00000064	TFA + Kids traffic campaign	$ 66,000	$ 60,000
ECOM00000038	Media buy for parents webinar campaign	$ 88,000	$ 57,550
ECOM00000057	Brand Voice and Positioning Development	$ 53,339	$ 48,490
ECOM00000077	Sextortion Campaign	$ 93,458	$ 44,962
ECOM00000046	Advertising services for education resources	$ 49,500	$ 42,289
ECOM00000095	2026 Brand Tracker	$ 104,500	$ 33,250
ECOM00000043	Coercive control awareness campaign	$ 22,000	$ 19,315
ECOM00000084	Be Connected NSW Seniors Card solus eDM and eNews	$ 16,500	$ 15,000
	TOTAL	**$ 801,297**	**$ 559,860**

- **We have achieved various efficiencies** including conversion of previously held labour hire positions to ongoing APS positions, implementing a new operating model and organisational structure to maximise delivery and alignment of functions.

Departmental Budget Summary – original 25/26 Budget	Full Year Budget %	Full Year Budget $'m
Regulatory Operations Division	1%	0.521
Investigations Branch	10%	6.107
Industry, Compliance and Enforcement Branch	8%	5.020
General Counsel	8%	4.987
Education Prevention & Inclusion Branch	12%	7.019
Strategy, Engagement and Research Branch	9%	5.611
Strategic Communications Branch	9%	5.213
Office of the Commissioner	3%	1.587
Technology & Strategy Division	2%	1.256
Technology, Data and Digital Enablement Branch	20%	12.086
Business Operations and Governance Branch	17%	9.983
Total	**100%**	**59.390**

Departmental Activity Budget Summary	Full Year Budget %	Full Year Budget $'m
Regulatory Functions	28%	16.635
Education, Outreach, Research, Engagement and public awareness	30%	17.843
Corporate and Technology	42%	24.912
Total	**100%**	**59.390**

Appendix 1.12: eSafety financial reporting

This appendix contains financial information on the operation of eSafety, presented in accordance with subsection 57(aa) of the ACMA Act.

	2025 $'000	2024 $'000
Departmental		
Operating expenses		
Employee benefits	29,239	23,727
Supplier expenses		
Consultants	2,182	1,071
Contractors	12,114	9,183
Outsourced services	6,179	1,386
IT and communications services	2,197	1,557
Travel costs	1,019	826
Other	2,822	2,218
Total supplier expenses	**26,513**	16,241
Total operating expenses	**55,751**	39,968
Capital purchases		
Internally developed software, leasehold improvement and PPE	43	730
Total capital purchases	**43**	730
Total departmental expenditure	**55,794**	**40,698**
Administered		
Grants expenditure	1,979	2,335
Supplier expenses		
Consultants		14
Contractors		2,404
Outsourced services		590
IT and communications services		711
Travel costs		11
Other		32
Total supplier expenses	**1,979**	3,762
Total administered expenditure	**1,979**	**6,097**

Departmental expenditure	2024-25	2023-24	Variance	Notes
TOTAL	**$55.794m**	**$40.698m**	**$15.096m**	
Employee benefits	$29.239m	$23.727m	$5.512m	Increase is expenditure related to new NPP's programs (including SMMA and internal legal and compliance) and the conversion of 27 contractors to APS staff. • 170 APS staff as at 30 June 2024 • 222 APS staff as at 30 June 2025
Consultants	$2.182m	$1.071m	$1.111m	Breakdown of $2.182m is at attachment A. 3 largest contracts spend in 2024-25: • $1.084m Contact Centre Solution Veritec Pty Ltd T/a Attura Cloud Business Solution) • $0.178m Subscription Consultancy Gartner Australasia Pty Ltd • $0.109m Technology Advisory Services Cyber CX Pty Ltd
Contractors	$12.114m	$9.183m	$2.931	Increase is part of Be Connected contractors moving from Admin to Dept exp in 25/26.
Outsourced services	$6.179m	$1.386m	$4.793m	3 largest expenditure areas: • $1.500m – Sydney fitout payment to ACMA • $2.379m – ACMA Corporate charges • $0.421m - BeConnected content
IT & Comms services	$2.197m	$1.557m	$0.640m	IT licencing and software
Travel costs	$1.019m	$0.826m	$0.193m	Overseas and domestic travel
Other	$2.822m	$2.218m	$0.604m	This includes: • $1.007m – Legal Fees • $0.247m – Media Relations • $0.333m – Marketing & Engagement • $0.138m – Graphic Design • $0.318m – Employee Development • $0.397m – Advertising
Capital purchases	$0.043m	$0.730m	(-$0.687m)	Purchase of Network Switches for Datacentre

Administered expenditure	2024-25	2023-24	Variance	Notes
TOTAL	**$1.979m**	**$6.097m**	**(-$4.118m)**	
Grants	$1.979m	$2.335m	(-$0.356m)	Payments were for: • Round 1 final payment $0.229m • Round 2 first payment $1.750m
Supplier expenditure	$0m	$3.762m	(-$3.762m)	The Be Connected program moved from administered expenditure to departmental expenditure in 2024-25.

9. Disaggregation of eSafety balances in the statements of comprehensive income

Note 9.1A Impact of eSafety on the Statement of Comprehensive Income

	Departmental (Excl. eSafety) $'000	eSafety $'000	Total $'000
NET COST OF SERVICES			
Expenses			
Employee benefits	66,369	29,239	**95,608**
Suppliers	26,288	26,513	**52,801**
Depreciation and amortisation	17,504	1,749	**19,253**
Finance costs	549	-	**549**
Impairment loss on financial instruments	203	-	**203**
Write-down and impairment of assets	37	54	**91**
Total expenses	110,950	57,555	**168,505**
Own-Source Income			
Own-source revenue			
Revenue from contracts with customers	308	1,114	**1,422**
Other revenue	142	-	**142**
Total own-source revenue	450	1,114	**1,564**
Gains			
Other gains	115	-	**115**
Total gains	115	-	**115**
Total own-source income	565	1,114	**1,679**
Net cost of services	(110,385)	(56,441)	**(166,826)**
Revenue from Government[1]	106,514	49,126	**155,640**
Surplus/(Deficit) attributable to the Australian Government	(3,871)	(7,315)	**(11,186)**
OTHER COMPREHENSIVE INCOME			
Items not subject to subsequent reclassification to net cost of services			
Changes in asset revaluation reserve	5,406	-	**5,406**
Total comprehensive income	1,535	(7,315)	**(5,780)**

[1] Departmental appropriation for eSafety is provided in the 2024-25 Budget process and credited to eSafety's Online Safety Special Account.

Area	Amount	Notes
Depreciation	$1.749m	Depreciation expense on the following assets: • Data governance, analytics and insights capability • Scalable Search • Sydney L1 fitout • Olympus Server • Fortinet Server • Microsoft Surface Laptops x 220 • Network Switches
Write down & impairment of assets	$0.054m	Write off of the depreciation balance left on the old Lenovo Laptops (90 units).
Revenue form contracts with customers	$1.114m	This comprised: • $0.840m – Department of Social Services – Transition Strategy - Technology Facilitated Abuse - Women and Children • $0.060m – Attorney Generals – Development of the National Law Enforcement Training Package • $0.150m - Dept of Education – Professional Learning Package - preventing cyberbullying for Chaplains and Student Wellbeing Officers • $0.055m – Pacific Community • $0.021m – APEC Program • (-$0.012m) – Unspent funding returned for Safety by Design in South East Asia
Surplus/ deficit	$7.315m	This represents: • $1.749m deprecation (non-appropriation) • $5.566m actual loss (covered by the approved loss). See note below for more detail regarding the loss.

Appendix 1.10: Outcome table

Appendix 1.10: Outcome table

This appendix contains information for both the ACMA and eSafety and shows how much was spent (on an accrual basis) on achieving the outcome by funding source.

Expenses for Outcome 1

Outcome 1: A communications and media environment that balances the needs of the industry and the Australian community through regulation, education and advice	Budget* 2024–25 $'000 (a)	Actual expenses 2024–25 $'000 (b)	Variation 2024–25 $'000 (a)-(b)
Program 1.3: eSafety Commissioner			
Administered expenses			
Ordinary annual services (Appropriation Act No. 1 and 3)	2,500	1,979	521
Administered total	**2,500**	**1,979**	**521**
Departmental expenses			
Special accounts (Online Safety Special Account – s72 *Enhancing Online Safety Act 2015*)	57,674	55,805	1,869
Expenses not requiring appropriation in the budget year[2]	725	1,749	(1,024)
Departmental total	**58,399**	**57,554**	**845**
Total expenses for Program 1.3	**60,899**	**59,533**	**1,366**

** Full-year budget, including any subsequent adjustment made to the 2024–25 budget at Additional Estimates.*
[1] Departmental appropriation includes the receipts retained under Section 74 of the PGPA Act 2013.
[2] Expenses not requiring appropriation in the Budget year are made up of depreciation expenses and amortisation expenses.

Area	Variance	Notes
TOTAL	**$1.366m**	
Administered variance	$0.521m	The budget of $2.500m reflected the previous phasing of the grant rounds. • A movement of funds, agreed in October 2025, has re-phased the budget to align with the new grant rounds. Actual expenses related to: • Round 1 final payments of $0.229m • Round 2 first payments of $1.750m.
Special accounts variance	$1.869m	Budget is what is in the 2024-25 PAES. It represents direct appropriation to eSafety and external revenue. Actual expenditure is seen in note 9: Disaggregation table. • $29.239m Employee benefits • $26.513m Suppliers • $ 0.054m write down of assets • **$55.805m Total**
Expenses not requiring appropriation - **variance**	(-$1.024m)	This is depreciation. Budget is what was in the 2024-25 PAES. This was updated to $1.724m in the 2025-26 PBS.

Media and advertising expenditure (page 109 in the AR)

Table 1.51: Expenditure on media advertising organisations, ACMA and eSafety, 2024–25

Organisation name	Purpose	Amount of payment ($ GST inc.)
ACMA expenditure		
Universal McCann	Public notices and general advertising	267,040
eSafety expenditure		
Universal McCann	Public Notices and general advertising	412,823
Total		**679,863**

Market research

Table 1.52: Expenditure on market research organisations, ACMA and eSafety, 2024–25

Organisation name	Purpose	Amount of payment ($ GST inc.)
ACMA expenditure		
Orima Research Pty Ltd	National Self-Exclusion Register research	120,805
The Social Research Centre Pty Ltd	Annual Consumer Survey and additional research services	159,129
Orima Research Pty Ltd	ACMA stakeholder survey 2023–25	16,500
Behavioural Insights (Australia) Pty Ltd	Dodgy devices part 2 – behavioural study	65,670
RMIT University	Mobile ethnography	119,864
Beverley Uther Research	Research services in domestic and family violence	5,000
ACMA total		**486,969**
eSafety expenditure		
Octopus Group Pty Ltd	Children and youth use of social media survey	15,136
eSafety total		**15,136**
Total		**502,105**

Expense	2024-25	2023-24	Variance	Notes
Media advertising	$412,823	$263,907	$148,916	Expenditure relating to general public notices and general advertising
Market research	$15,136	$566,620	(-$551,484)	Expenses in 2023-24 comprised two major projects (below) where there was none in 2024-25: • $0.195m Deakin University for the Boys to Men project • $0.353m KPMG for user-centred research and design for the TFA Service

*All figures are GST inclusive

Consultants Expenditure (page 68 in the AR)

Consultants

The ACMA and eSafety engage consultants to provide specialised services when the capability or capacity to perform these in-house is not available, or where there is a requirement for independent advice or the development of intellectual output to assist with decision making. The majority of consultants were engaged following an open approach to market and use of panel arrangements. The main categories for consultancies in 2024–25 were research and general advice.

During 2024–25, 27 new reportable consultancy contracts were entered into for the ACMA and eSafety, involving total actual expenditure of $2,659,211 (Table 1.15). In addition, 13 ongoing reportable consultancy contracts were active during the period for the ACMA and eSafety, involving total actual expenditure of $818,256 (Table 1.16).

Table 1.15: Number and expenditure on new consultancy contracts, 2024–25

	Number of contracts	Expenditure $ (GST inc.)
ACMA	10	552,412
eSafety	17	2,106,799
Total	**27**	**2,659,211**

This table includes both administered and departmental expenditure on consultancies.

Table 1.16: Number and expenditure on ongoing consultancy contracts, 2024–25

	Number of contracts	Expenditure $ (GST inc.)
ACMA	10	744,501
eSafety	3	73,755
Total	**13**	**818,256**

This table includes both administered and departmental expenditure on consultancies.

Table 1.17: Total expenditure on consultancy contracts, 2021–22 to 2024–25

Year	New consultancies $ (GST inc.)	Continued consultancies $ (GST inc.)
2021–22	2,390,157	1,434,342
2022–23	2,524,785	1,958,055
2023–24	1,719,045	1,611,145
2024–25	2,659,211	818,256

Table 1.18: Organisations receiving a share of reportable consultancy contract expenditure, 2024–25

Name of organisation	Organisation ABN	Expenditure $'000 (GST inc.)
Veritec Pty Ltd T/a Atturra Cloud Business Solutions	21166493394	1,084,363
The Social Research Centre Pty Ltd	91096153212	363,140
Gartner Australasia Pty Ltd	69003708601	177,760
The Social Research Centre Pty Ltd	91096153212	159,129
Omnipoll Pty Ltd	45606468044	156,996

Consultants	2024-25	2023-24	Variance	Notes
New contracts - number	17	5	12	Breakdown is at attachment A 3 largest contracts spend in 2024-25: • **$1.084m** Contact Centre Solution Veritec Pty Ltd T/a Attura Cloud Business Solution • **$0.178m** Subscription Consultancy Gartner Australasia Pty Ltd • **$0.109m** Technology Advisory Services Cyber CX Pty Ltd
New contracts - expenditure	$2,106,799	$216,816	$1,889,983	
Ongoing contracts – number	3	8	(-5)	Breakdown is at attachment A Contracts spend in 2024-25: • $0.025m Teacher Professional Learning Module for Lower Primary Early Childhood Australia Inc. • $0.049m eSafety Website UX Review Ellis Jones Consulting
Ongoing – expenditure	$73,755	$559,188	(-$485,433)	
TOTAL	**$2,180,554**	**$776,004**	**$1,404,550**	

*All figures are GST inclusive

Note - Difference in Figures p68 and Appendix 1.12

Consultant's comparison	GST exclusive	GST inclusive	Notes
Expenditure in appendix 1.12	$2.18m	**$2.40m**	The Appendix table is GST exclusive. Data is sourced from the Finance system and is based on accrual figures. The Consultant's table is GST inclusive. Data is sourced from the procurement system and is based on payments made (not accruals).
Expenditure in Consultants note		New $2.11m Ongoing $0.07m **Total $2.18m**	
Variance		**$0.22m**	

Non - consultants expenditure (page 69 in the AR)

Non-consultants

The ACMA and eSafety procure goods and services to deliver agency outcomes. During 2024–25, 149 new reportable non-consultant contracts were entered into for the ACMA and eSafety involving total actual expenditure of $8,545,534 In addition, 197 ongoing reportable non-consultant contracts were active during the period for the ACMA and eSafety, involving total actual expenditure of $42,161,334.

Table 1.19: Number and expenditure on new non-consultancy contracts, 2024–25

	Number of contracts	Expenditure $ (GST inc.)
ACMA	69	3,119,355
eSafety	76	5,426,179
Total	**145**	**8,545,534**

This table includes both administered and departmental expenditure on contractors.

Table 1.20: Number and expenditure on ongoing non-consultancy contracts, 2024–25

	Number of contracts	Expenditure $ (GST inc.)
ACMA	119	28,061,697
eSafety	78	14,099,637
Total	**197**	**42,161,334**

This table includes both administered and departmental expenditure on contractors.

Table 1.21: Organisations receiving a share of reportable non-consultancy contract expenditure, 2024–25

Name of organisation	Organisation ABN	Expenditure $'000 (GST inc.)
Evolve FM Pty Ltd Facilities Trust Payment only	52605472580	10,524,333
Talent International (ACT) Pty Ltd	95121819305	4,395,243
IVE Group Australia Pty Ltd	58000205210	2,707,338
Dataworks Group Limited (formerly IXUP Limited)	85612182368	2,681,608
Balance Consulting Services Pty Ltd	31636099039	2,416,417

Note: This table includes contractors along with all non-consultancy contracts.

Non - Consultants	2024-25	2023-24	Variance	Notes
New contracts - number	76	81	(-5)	Breakdown is at attachment B Top suppliers spends in 2024-25: • $4,395,243 - Talent International (ACT) Pty Ltd • $2,416,417 - Balance Consulting Services Pty Ltd • $1,659,144 - Clicks Recruit (Australia) Pty Ltd • $1,039,173 - Hays Personnel Services (Australia) • $946,934 - Servegate Australia Pty Ltd • $767,947 - Bluefin Resources Pty Ltd • $534,025 - Data #3 Limited • $500,706 - Dynamo Recruitment Pty Ltd • $412,823 - Universal McCann • $408,040 - Australian Government Solicitor
New contracts - expenditure	$5,426,179	$4,105,937	$1,320,242	
Ongoing contracts – number	78	112	(-34)	
Ongoing – expenditure	$14,099,637	$14,137,699	(-$38,062)	
TOTAL	**$19,525,816**	**$18,243,636**	**$1,282,180**	

Contractors expenditure (page 70 in the AR)

Contractors

The ACMA and eSafety engage contractors to perform specialised duties under their direction and supervision. The policy for selecting and engaging contractors, including the use of standing panel arrangements, is in accordance with the CPRs and based on the core principle of achieving value for money.

Table 1.22: Total expenditure on contractors, 2021–22 to 2024–25

Year	ACMA $ (GST inc.)	eSafety $ (GST inc.)	Total $ (GST inc.)
2021–22	6,682,225	15,658,681	22,340,906
2022–23	3,001,567	20,405,951	23,407,518
2023–24	2,380,369	18,243,636	20,624,005
2024–25	2,391,319	13,522,544	15,913,863

This table includes both administered and departmental expenditure on contractors. Contractor expenditure reported in this table is included in total non-consultancy expenditure in the above section.

Contractors	2024-25	2023-24	Variance	Notes
Expenditure	$13,522,544	$18,243,636	(-$4,721,092)	46 Contractors at 30 June 2024 38 Contractors at 30 June 2025 We have converted 27 contract roles to APS roles

*All figures are GST inclusive

Note – Difference in Figures p70 and Appendix 1.12

Contractor's comparison	GST exclusive	GST inclusive	Notes
Expenditure in appendix 1.12	$12.114m	$13.325m	The Appendix table is GST exclusive. Data is sourced from the Finance system and is based on accrual figures.
Expenditure in Contractors note		$13.523m	The Consultant's table is GST inclusive. Data is sourced from the procurement system and is based on payments made (not accruals).
Variance		**$0.198m**	

Supplier expenditure YTD

Financial Report for the Period Ended: April 2026

E-Safety Financial Report by Natural account

Section Summary	YEAR TO DATE			FULL YEAR		
	ACTUALS	BUDGET	VARIANCE	FULL YEAR FORECAST	FULL YEAR BUDGET	VARIANCE
	$000	$000	$000	$000	$000	$000
EXPENSES						
Employee Expenses						
Employee Salaries	30,934	30,899	-35	37,394	37,564	170
Employee Development	184	221	37	313	286	-27
Employee Sundry Costs	247	182	-65	297	238	-59
Total Employee Expenses	31,365	31,302	-63	38,004	38,088	84
Supplier Expenses						
Contractor & Temporary Staffing Costs	5,652	5,828	175	6,554	6,868	313
Contracts	3,608	4,105	497	4,165	4,427	261
Consultants	1,184	1,380	192	1,615	1,555	-60
Domestic Travel	446	445	-1	526	530	4
International Travel	152	152	-15	192	152	-40
Media & Publishing	648	955	307	808	1,066	258
Advertising and Marketing	174	88	-85	352	267	-85
IT Equipment and Support	1,329	1,560	231	1,867	1,857	-9
Supplier Sundry Cost	5,350	4,697	-634	5,751	5,266	-485
Total Supplier Expenses	18,543	19,209	666	21,832	21,988	157
TOTAL EXPENSES	49,908	50,512	603	59,836	60,076	241

Employee expenses	31.354m
Contractors	5.65m
Consultants	1.184m
Suppliers	5.35m
Media & publishing	658k
Advertising & marketing	147K
Domestic travel	446k
International travel	152k
YTD expenditure	49.908m

Operating Loss

eSafety's 2024-25 financial position was a loss of **$5.566m (**this excludes depreciation).

eSafety's 2024-25 **comprehensive income position** was a loss of **$7.315m (**this includes depreciation).

eSafety operating loss	$5.566m
eSafety depreciation	$1.749m
Comprehensive loss position	**$7.315m**

The ACMA's and eSafety's combined **comprehensive income position** was a loss of **$5.780m**

eSafety comprehensive loss position	$7.315m
ACMA comprehensive income position	$1.535m
Comprehensive loss position	**$5.780m**

Approval was provided for the ACMA and eSafety to make a **$4.878m** operating loss in the 2024-25 financial year. eSafety projected a loss of $5.656m which was partially offset by an expected ACMA surplus of $0.778m.

The loss was **funded via use of eSafety's special account balance.** This balance has been contributed to since the commencement of the then *Children's eSafety Commissioner* which accrued as a result of funding received but not spent when the commission was initially established.

The use of the special account balance in 2024-25 to cover the loss was to:

- Offset the TFA support service project funding profile
  - The TFA Support Service project was originally funded from 2022-23 for four years.
  - To appropriately implement the project, considerable scoping, research and consultation was required for this world's first scheme.
  - The associated construct of an expert foundation knowledge, resources, and IT requirements were challenging and not in line with the Govt. funding profile.
  - eSafety has ensured that the total funding provided will be utilised on the project, however expenditure will be profiled differently to original forecasts.
- Manage **one off expenditure** relating to the implementation of new regulatory schemes
- Manage the **increased legal costs** associated with several high-profile court processes
- Provide resources to assist in the **review of the Online Safety Act**
- Manage the **increased scrutiny, public profile and requests** on all areas of eSafety
  - including FOI's and extensive media enquiries

ACMA and eSafety came in under the approved loss of $4.878m in the 2024-25 financial year.

Loss position in the annual report:

9. Disaggregation of eSafety balances in the statements of comprehensive income

Note 9.1A Impact of eSafety on the Statement of Comprehensive Income

	Departmental (Excl. eSafety) $'000	eSafety $'000	Total $'000
OTHER COMPREHENSIVE INCOME			
Items not subject to subsequent reclassification to net cost of services			
Changes in asset revaluation reserve	5,406	-	5,406
Total comprehensive income	1,535	(7,315)	(5,780)

2026-27 PBS Budget breakdown

2026-27 PBS table	2025-26 Estimated actual $m	2026-27 Budget $m	2027-28 Forward estimate $m	2028-29 Forward estimate $m	2029-30 Forward estimate $m
Program 1.3: Office of the eSafety Commissioner					
Administered expenses					
Ordinary annual services					
Appropriation Bill (No. 1)	1.750	3.500	-	-	-
Administered total	**1.750**	**3.500**	**-**	**-**	**-**
Departmental expenses					
Departmental appropriation	66.474	65.653	57.708	54.467	55.368
s74 External Revenue	0.390	0.300			
Special Account					
Appropriation receipts	59.386	58.580	50.636	47.395	48.296
less expenses made from appropriations credited to special accounts	-59.386	-58.580	-50.636	-47.395	-48.296
Expenses not requiring appropriation in the Budget year	1.687	0.514	0.373	0.012	-
Departmental total	**68.551**	**66.467**	**58.081**	**54.479**	**55.368**
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**

2026-27 PBS table breakdown	2025-26 Estimated actual $m	2026-27 Budget $m	2027-28 Forward estimate $m	2028-29 Forward estimate $m	2029-30 Forward estimate $m
Grants	2.500	2.500			
Grants - 2025-26 Movement of funds	-0.750	1.000			
Administered Total	**1.750**	**3.500**	**0.000**	**0.000**	**0.000**
Original base funding	10.309	10.309	10.309	10.309	10.309
Additional ongoing base funding Budget 2023-24	24.382	24.765	24.765	24.765	24.765
SMMA funding	13.163	13.260	12.418	12.283	12.283
Other impacts (including indexation)	0.809	1.165	1.774	2.159	2.810
Savings from External Labour - extension	-0.140	-0.129	-0.909	-0.566	
Savings from External labour, Advertising, Travel & Legal expenses	-1.022	-0.620			
Savings from 2025 Election Commitment	-0.908				
Savings from 2025-26 MYEFO		-1.990	-1.765	-1.469	
Saving from 2026-27 Budget		-0.105	-0.090	-0.086	-1.871
Total Base funding	**46.593**	**46.655**	**46.502**	**47.395**	**48.296**
NPP eSafety General awareness Initiative	0.100	0.100			
NPP Be Connected	4.034	4.082	4.134		
NPP National Strategy to Prevent Child Sexual Abuse	0.644	0.656			
NPP TFA Technical Support	5.600	5.434			
NPP Protecting Australians Online	1.633	1.653			
NPP Internal legal and Compliance	0.782				
Total NPP funding	**12.793**	**11.925**	**4.134**	**0.000**	**0.000**
Total Departmental Appropriation receipts	**59.386**	**58.580**	**50.636**	**47.395**	**48.296**
ACMA direct appropriation funding	8.909	8.909	8.909	8.909	8.909
Less ACMA capital funding	-1.821	-1.837	-1.837	-1.837	-1.837
Total ACMA funding	**7.088**	**7.072**	**7.072**	**7.072**	**7.072**
Expenses not requiring appropriation (depreciation)	**1.687**	**0.514**	**0.373**	**0.012**	
s74 External revenue	**0.390**	**0.300**			
Departmental Total	**68.551**	**66.467**	**58.081**	**54.479**	**55.368**
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**

NPP impacts	2025-26	2026-27	2027-28	2028-29	2029-30
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**
Change in funding per year		**-0.334**	**-11.886**	**-3.602**	**0.889**
Reduction in NPP by year:					
Administered - Grants			-3.500		
NPP eSafety General awareness Initiative			-0.100		
NPP Be Connected				-4.134	
NPP National Strategy to Prevent Child Sexual Abuse			-0.656		
NPP TFA Technical Support			-5.434		
NPP Protecting Australians Online			-1.653		
NPP Internal legal and Compliance		-0.782			
Total NPP funding loss by year		**-0.782**	**-11.343**	**-4.134**	

Terminating Measures

- The only terminating measure this year is the Internal Legal and Compliance ($0.782m)

2026-27 PBS	2025-26 Estimated actual	2026-27 Budget	2027-28 Budget	2028-29 Budget	2029-30 Budget
Grants	2.500	2.500			
Grants - 2025-26 Movement of funds	-0.750	1.000			
Administered Total	**1.750**	**3.500**	**0.000**	**0.000**	**0.000**
Original base funding	10.309	10.309	10.309	10.309	10.309
Additional ongoing base funding Budget 2023-24	24.382	24.765	24.765	24.765	24.765
SMMA funding	13.163	13.260	12.418	12.283	12.283
Other impacts (including indexation)	0.809	1.165	1.774	2.159	2.810
Savings from External Labour - extension	-0.140	-0.129	-0.909	-0.566	
Savings from External labour, Advertising, Travel & Legal expenses	-1.022	-0.620			
Savings from 2025 Election Commitment	-0.908				
Savings from 2025-26 MYEFO		-1.990	-1.765	-1.469	
Saving from 2026-27 Budget		-0.105	-0.090	-0.086	-1.871
Total Base funding	**46.593**	**46.655**	**46.502**	**47.395**	**48.296**
NPP eSafety General awareness Initiative	0.100	0.100			
NPP Be Connected	4.034	4.082	4.134		
NPP National Strategy to Prevent Child Sexual Abuse	0.644	0.656			
NPP TFA Technical Support	5.600	5.434			
NPP Protecting Australians Online	1.633	1.653			
NPP Internal legal and Compliance	0.782				
Total NPP funding	**12.793**	**11.925**	**4.134**	**0.000**	**0.000**
Total Departmental Appropriation receipts	**59.386**	**58.580**	**50.636**	**47.395**	**48.296**
ACMA direct appropriation funding	8.909	8.909	8.909	8.909	8.909
Less ACMA capital funding	-1.821	-1.837	-1.837	-1.837	-1.837
Total ACMA funding	**7.088**	**7.072**	**7.072**	**7.072**	**7.072**
Expenses not requiring appropriation (depreciation)	**1.687**	**0.514**	**0.373**	**0.012**	
s74 External revenue	**0.390**	**0.300**			
Departmental Total	**68.551**	**66.467**	**58.081**	**54.479**	**55.368**
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**

SMMA Funding

Key Points

- Funding of **$45.651m** over **four years** was provided from 2024-25. **$12.3m** per year ongoing funding from 2028-29.
- **40** ongoing ASL
- **Note in budget paper:**
  - **Social Media Age Limits** – a cross-agency initiative to establish a minimum age of access to social media. This measure provided **$45.7 million over 4 years** from 2024–25 (and **$12.3 million per year ongoing**) for eSafety to provide regulatory oversight and enforcement functions. The measure also provides 11.5 additional Average Staffing Level (ASL) in 2024–25 and 40 additional ASL each year from 2025–26 onwards.

Summary	2024-25	2025-26	2026-27	2027-28	2028-29 Ongoing
Departmental funding	$3.810m	$13.163m	$13.260m	$12.418m	$12.283m
Capital funding		$3.000m			
Total	**$3.810m**	**$16.163m**	**$13.260m**	**$12.418m**	**$12.283m**
ASL	11.5	40.0	40.0	40.0	40.0
Contractors	1.0	5.0	5.0	2.5	2.5
Total	**12.5**	**45.0**	**45.0**	**42.5**	**42.5**

- eSafety **has fully spent it funding allocation against SMMA in 2024-25** and is budgeted to fully spend the 2025-26 budget allocation.

	2025-26 GST inclusive	2026-27 GST inclusive	2027-28 GST inclusive	Total GST inclusive
SMAA evaluation contract amount	$765,791	$651,442	$163,105	**$1,580,338**

A recent QON asked:
Q: What is the expected cost of the two-year longitudinal survey as identified in the Statement of Work: Evaluation of the Social Media Age Restriction?
A: $1,460,839 GST inclusive
This answer did not include the delivery of a component funded by the Institute of Criminology. This amount is included in the table above.

Previous Financial Years results

As per the **Appendixes** in the Annual Report

Financial Year	Departmental Spend	Administered Spend	TOTAL	Change from previous year
2015-16	$10.440m	$0.856m	**$11.296m**	-
2016-17	$11.915m	$1.273m	**$13.188m**	26%
2017-18	$13.298m	$7.199m	**$20.497m**	55%
2018-19	$15.572m	$6.833m	**$22.405m**	9%
2019-20	$18.648m	$5.359m	**$24.007m**	7%
2020-21	$23.824m	$6.342m	**$30.166m**	25%
2021-22	$38.953m	$8.888m	**$47.841m**	59%
2022-23	$47.453m	$6.209m	**$53.662m**	12%
2023-24	$40.699m	$6.096m	**$46.795m**	-13% *
2024-25	$55.793m	$1.979m	**$57.773m**	23%

Note: Difference in the 2022-23 to 2023-24 Departmental spend is in relation to the ACMA corporate cost funding. This commenced being appropriated directly to the ACMA in 2023-24 (as a result of the funding review).

Funding background

- When eSafety was established in 2015 its baseline funding was **$10.3m.**
- Over the FYs that followed to support ongoing growth the vast majority of eSafety's available funding was provided by terminating measures leading to an ***average operating budget of around $50m*** per year (prior to Social Media Minimum Age NPP)
- Many of these terminating measures were set to expire in 2023-24 dropping eSafety's budget to $21m and then down to $10.3m in the outyears.
- As a result of a **funding review in 2023** eSafety's baseline operating budget was quadrupled from **$10.3m to $42m ongoing** from 2023-24. It was further increased with the passage of the Social Media Minimum Age Amendment to approximately ***$54m ongoing***
- eSafety's total budget comprises this ongoing funding and terminating funding initiatives such as the TFA Support Service and a Grants program.

Internal Budget Allocation

- **We work effectively within the budget we have been provided** focusing our allocation of resources in accordance with our functions under the Online Safety Act, our Corporate Plan objectives and the **Minister's Statement of Expectations**.
- Emphasis is on **regulatory operations** including complaint handling and investigations, compliance and enforcement activities as well as awareness raising, education and outreach.
- **We will continue to work with the Department** on any future budget requirements.

s83

Page 144 in the annual report

Potential breach of Section 83 of the Constitution

Section 83 of the Constitution provides that no money shall be drawn from the Treasury of the Commonwealth except under appropriation made by law.

For the 2024-25, it has been identified that five eSafety invoices totalling $153,518.07 were incorrectly paid out of the administered account.

This resulted from an administrative error and occurred in the transition of funding for the eSafety BeConnected program from administered funding to ongoing departmental funding at the beginning of the financial year. Inadvertently the Purchase Orders for the contracts affected were not updated ahead of the 1 July 2024 start date.

This is a potential breach of section 83 of the Constitution given the requirement is that funds can only be drawn from the Consolidated Revenue Fund (CRF) with a valid and approved appropriation. The ACMA have taken remedial actions to address the matter.

eSafety breached s83 of the constitution in the 2024-25 financial year.

- The error was administrative in nature and occurred in the transition of funding for the eSafety Be Connected program from administered funding to departmental funding.

- From **1 July 2024** the Be Connected program is funded from departmental appropriations, prior to this **since 2017** it was funded by administered appropriation.

    - The administrative oversight related to existing purchase orders for contracts in place for Be Connected suppliers were not updated to be paid from departmental funds from July 2024.
    - In July 2024, **five invoices totalling $153,518.07** were made from administered funding via these purchase orders.
    - Once this was identified, **the payments were reversed** and applied back to the administered account.

Section 83 of the Constitution provides that no money shall be drawn from the Treasury of the Commonwealth except under appropriation made by law.

- In this instance there was no valid appropriation available to draw funds from in the administered account.
- As a result, this has been identified as a breach of section 83 of the Constitution given funds can only be drawn from the Consolidated Revenue Fund (CRF) with a valid appropriation.

The breach was reported to the accountable authority, was registered on ACMA"s Breach Register and reported to the Audit and Risk Committee.

- It was deemed that the breach was **not a systemic breach**, occurred once and was made in error.
- Additional steps have been implemented to ensure this does not occur again.

Special account

- Set out in Section 190 of the Online Safety Act
- ACMA and eSafety report as a single financial entity
- Specified departmental and administered funds for eSafety are accredited to the Online Safety Special Account
- The Special Account is administered by the ACMA, but any amount debited requires the written approval of the Commissioner (delegated out by financial delegations)
- It allows unused funds from the FY to be rolled over for use by seeking approval from the Minister for Finance (operating loss)
- Funds may accrue due to delays in recruitment and procurement spend or changes to delivery timelines and may be used for the purposes outlined under Section 190 of the Online Safety Act.

Austender media questions

Media response in regard to reporting of eSafety contractor costs

- I would also like to take the opportunity to correct the record that the figures reported recently in media articles of payments made to contractors and temporary staff were far higher than the actual amount paid by eSafety.
- These figures quoted appear to have used total contract value amounts published on AusTender.
- This amount reflects the estimate of the total value of a contract when a contract, or purchase order, is raised and is often very different to the actual amount paid for services.
- For example, figures quoted in respect of payments made for a senior executive assistant were incorrectly quoted in the media article as being more than 50% higher ($86,000 more) than the actual payments made.
- Further, a figure quoted in respect of payments made for an Assistant Manager Indigenous programs was incorrectly quoted as being paid **$4,694** per day when in fact the daily rate was **$950 per day** (20% of that figure) which was in accordance with market rate for that skillset.
- This figure was incorrectly extrapolated from a total Aus Tender contract value of $314,545 over a 67-day contract period. This contract period was published incorrectly.
- There were numerous other inaccuracies in respect of the payments made to other contractors.
- Whenever engaging contractors and labour hire eSafety are highly focussed on ensuring a competitive and **value for money process** is always undertaken and consistent with the broader Commonwealth procurement guidelines.

Staffing

Staffing	As at 30 April 2026	*As at 30 April 2025*	Variance	Percentage change
APS (FTE)	236	*194*	42	22% increase
Contractors (FTE)	20	*44*	-24	55% decrease
Total	**256**	**238**	**18**	**8% increase**

- The growth in APS staffing numbers represents an increase in staff associated with new programs, primarily the SMMA NPP.
- The reduction in contractors represents the conversion of contractor roles to APS roles, as per the Government's Strategic Commissioning Framework, and the conclusion of some contracts.

Wellbeing and Strategic HR

- eSafety has 1 FTE attributed to Strategic HR functions.
    - This role encompasses a broad range of strategic HR functions including staff wellbeing, culture and workforce planning.
- eSafety does not have any staff solely dedicated to diversity, equity and inclusion (DEI) programs or change management.
- ACMA leads the development of diversity, equity and inclusion strategies and policies for ACMA and eSafety.
    - specific DEI questions should be referred to the ACMA
- List of external DEI related speakers since 1 July 2024:

Name of Company / Speaker	Date	Amount Paid (GST inclusive)	Event
Acknowledge This Rhys Paddick	24 July 2024	$5,500	Indigenous Training for Staff
Company: Minus 18	2 Sept 2024	$1,188	Wear it Purple Day talk
Nina Jankowicz	6 Sept 2024	$0	All staff talk
Dr Leonie Maria Tanczer	2 Oct 2024	$0	Online presentation – topic: Internet of Things and Family, Domestic and Sexual Violence training
Act For Kids Thomas Rhodes	6 Nov 2024	$0	Information session to eSafety staff on harmful sexual behaviour in young people related to AI companions
Reconciliation NSW Joshua Gilbert	11 July 2025	$825	NAIDOC week speaker

Census results & wellbeing

- eSafety has a strong overall culture, with **positive engagement at 80%** - above the APS average.
- Reported rates on bullying and harassment are low, with 93% not experiencing bullying or harassment and 97% not experiencing discrimination.
- **Our culture strongly supports integrity (89%), respect (84%) and inclusion (84%),** which are key protections against poor behaviour.
- eSafety staff are highly committed - **94% feel committed to eSafety's mission** of keeping Australians safe online and 95% are willing to go the extra mile.
- We recognise workload pressures in some areas and are actively managing prioritisation and resource allocation. Our census action plan outlines how we are doing this at all levels of the organisation.
- We continue to prioritise staff wellbeing. This is particularly important given the nature of our regulatory scope and staff exposure to potentially traumatic material and challenging interactions with complainants.
- To support the emotional and psychological demands these roles, we provide a comprehensive range of proactive supports from induction through to when staff leave eSafety. These measures are designed to promote wellbeing and ensure staff are equipped to manage the unique challenges of our work. Examples include:
    - **Technology solutions** to reduce expose to distressing and sensitive content
    - **Regular proactive wellbeing check ins** for staff in high-risk roles
    - **Psychosocial training** and coaching for leaders
    - **Regular training on a range of wellbeing topics** (e.g. vicarious trauma, psychological first aid)
    - **Strong focus on peer support**
    - **Pre-employment psychological screening** and exit debriefs
    - **Working with psychosocial risk experts** to ensure jobs are designed appropriately and support wellbeing.

Evaluation of Social Media Minimum Age

Academic Advisory Group

Members of the Lead Academic Partner

- Professor Jeff Hancock, Stanford University Social Media Lab
- Dr Sunny Xun Liu, Stanford University Social Media Lab
- Dr Anja Stevic, Stanford University Social Media Lab
- Dr Angela Yuson Lee, Stanford University Social Media Lab
- Dr Y. Anthony Chen, Stanford University Social Media Lab
- Zacariah Smith-Russack, Stanford University Social Media Lab

Members of the Academic Advisory Group – 6 Australian

- Distinguished Professor Bronwyn Carlson, Head of Critical Indigenous Studies, Macquarie University
- Professor Peter Etchells, School of Psychology, Bath Spa University
- Professor Katherine Keyes, Mailman School of Public Health, Columbia University
- Distinguished Professor Mitch Prinstein, Co-Director of the Winston Center for Technology and the Developing Mind, University of North Carolina, and Chief Science Officer, American Psychological Association.
- Professor Jo Robinson, Professorial Fellow and Director, Centre for Youth Mental Health, University of Melbourne
- Professor Susan Sawyer, Chair of Adolescent Health, University of Melbourne, and Director, Centre for Adolescent Health, Royal Children's Hospital
- Professor Julian Sefton-Green, School of Education, Deakin University
- Associate Professor Aliza Werner-Seidler, Black Dog Institute, University of New South Wales
- Professor Amanda Third, Professorial Research Fellow and Co-Director, Young and Resilient Research Centre, Western Sydney University
- Associate Professor, Munmun De Choudhury, Director of Social Dynamics and Well-Being Laboratory, and Co-Lead of Children's Healthcare of Atlanta Pediatric Technology Center, Georgia Institute of Technology
- Professor Amy Orben, Programme Leader Track Scientist at the MRC Cognition and Brain Sciences Unit, University of Cambridge

How were they selected?

Key talking points – Academic Advisory Group and evaluation

- **Independent expert oversight:** The Advisory Group provides expert advice, peer review and guidance across design, analysis and publication—bringing global expertise in online harms, social media and youth wellbeing.
- **Transparent and rigorous selection:** Members (including Stanford) were chosen through a competitive Expression of Interest process, with strong assessment criteria and conflict of interest checks reviewed by a multi-disciplinary committee.
- **Strong governance and integrity safeguards:** All members must sign agreements, disclose and manage conflicts of interest, and commit to a neutral, evidence-based approach to ensure credibility of the evaluation.
- **Defined roles for impact:** The Lead Academic Partner plays a central role in designing the evaluation and analysing data, while the Advisory Group provides independent advice, peer review and supports dissemination.
- **High-quality field of applicants:** eSafety received 32 Advisory Group applications and 5 for Lead Academic Partner, with Stanford unanimously selected for its leading expertise in youth wellbeing and social media harms.

Back pocket summary

Purpose

- To evaluate the implementation and impacts of Australia's Social Media Minimum Age legislation on:
    - Young people (10–16)
    - Parents and families
    - Community attitudes and dynamics
- Designed to assess both intended and unintended outcomes over time.
- The approach recognises that population-level mental health change is a long-term outcome (5+ years) and therefore focuses on early indicators known to influence wellbeing, such as sleep, social connection and social comparison

Costs

- Total costs over 3-years is expected to be $1.6m
- This includes:
    - Approx $ 1.46 million for the survey. The fieldwork vendor is Social Research Centre.
    - Approx $128K to facilitate data linkage of cohort data with administrative datasets. This provider is Australian Institute of Family Studies (they are an accredited data linkage provider)
    - Approx $30K for data custodian costs. The custodian is Services Australia
    - Approx $15K to Australian Institute of Family studies for ethical review.
    - Budget is also allocated to cognitive testing of research instruments, and editing and publishing costs

Study Design

- Mixed-methods, longitudinal evaluation over two years
- Sample: ~4,121 parent–child dyads at baseline
- Five survey waves (Nov 2025 – Nov 2027)
- Combines:
    - Paired parent–child surveys
    - Optional passive smartphone usage data (opt-in)
    - Qualitative research (focus groups, interviews, diary studies)
    - Optional linkage to administrative data (e.g. education and health datasets)

Key Evaluation Questions – Summary

- ✓ Levels of awareness, compliance and circumvention
- ✓ Changes in digital practices and exposure to online harms
- ✓ Impacts on psychological, social and physical wellbeing
- ✓ Effects on family dynamics and parental mediation
- ✓ Shifts in community attitudes and social norms
- ✓ Differential impacts across groups, including Aboriginal and Torres Strait Islander families

Mental health measures

- We have a large number of validated measures in the survey regarding mental health and wellbeing.
- For example, we have the K6 (Kessler 6) which measures psychological distress, the Warwick-Edinburgh Mental Wellbeing Scale, which measures the feeling and functioning aspects of wellbeing, the Strengths and Difficulties Questionnaire which measures externalising symptoms (i.e. those that you can spot) of mental health such as emotional, social, and behavioural symptoms.
- These are self-report and/or parent report and measured at each timepoint.

We then have data linkage which will link consenting participants data with their Medicare and PBS and NAPLAN.

Methodological Strengths

- Large, nationally distributed cohort
- Paired parent–child design
- Use of validated survey instruments supplemented by tailored measures
- Oversampling of Aboriginal and Torres Strait Islander participants
- Integration of quantitative, qualitative and objective usage data
- Academic peer review and independent oversight

Limitations (Acknowledged)

- Expected attrition across five waves
- Final-wave sample size may limit statistical power for some subgroup analyses
- While we acknowledge the limitations of self-report the study does use a wide range of validated measures deployed longitudinally. These instruments have been scientifically tested to ensure they accurately, reliably, and consistently measure the specific constructs they are designed to assess.
- The use of validated measures is strongly recommended in longitudinal research because it provides a stable and credible foundation for comparing data collected across multiple time points.

Governance, Ethics and Independence

- eSafety is the lead agency for the evaluation
- Lead Academic Partner: Stanford Social Media Lab
- Supported by an independent Academic Advisory Group
- Ethics approval through AIFS HREC
- Strong safeguards for consent, assent, privacy and data security
- Participation in enhanced data collection is voluntary and opt-in

Dissemination

- Findings to be released through:
    - Public reports
    - Peer-reviewed publications
    - Stakeholder briefings and engagement

- eSafety has prior visibility of publications but does not restrict academic independence
- Evaluation designed to inform statutory review and future implementation decisions
- Report schedule:
    - Baseline findings released earlier this year
    - Wave 1 report comparing first 4 months with baseline – July
    - Wave 2 – End of year

Priority Outcome Domains

1. Implementation
    - Child and parent circumvention and compliance
    - Reported at 3, 6, 12 and 24 months to support early oversight of implementation effectiveness
2. Children's Digital Lives – Norms and Pressure
    - Children's norms and attitudes toward social media
    - Pressure to participate in social media
    - Early reporting from 6 months, with continued tracking through 24 months
3. Parents, Families and Communities
    - Parental norms and perceived social pressure
    - Parental stress
    - Family communication, cohesion and conflict (including conflict around online activities)
    - Selected indicators reported early, with fuller reporting through 12 and 24 months
4. Children's Digital Lives – Online Harms
    - Exposure to online harms
    - Problematic or excessive social media use
    - Social comparison
    - Primarily reported at 12 and 24 months, reflecting expected time needed for behavioural change to emerge
5. Impact on Children's Wellbeing and Functioning
    - Physical wellbeing: sleep quality, sleep quantity, offline activities
    - Psychological wellbeing: mental wellbeing and distress indicators
    - Social wellbeing: school connectedness, peer relationships, loneliness
    - Body image
    - Some early indicators tracked from 6 months, with core wellbeing outcomes reported at 12 and 24 months

Key Messages

- The evaluation is deliberately staged, matching expected timing of change
- Early reporting focuses on implementation, norms and pressure
- Wellbeing outcomes are tracked using validated measures, with appropriate expectations about timing
- This ensures Government has early visibility of trends while building a robust evidence base for the statutory review

Communications guidelines – Advisory group

The guidelines provided to members of the Academic Advisory Group outline their roles and expectations, including the requirement to act in a manner that does not compromise, or appear to compromise, the objectivity of the evaluation. Specifically:

- Members act as part of an independent academic advisory group supporting a rigorous and impartial evaluation.
- Members do not speak on behalf of the evaluation, the Advisory Group, eSafety, or the Australian Government unless explicitly authorised.
- Members are free to speak publicly but are requested to clearly distinguish personal views from their advisory role and to be transparent about the limitations of the evidence base.
- Members are requested to emphasise that the evaluation will consider both positive and negative outcomes and to avoid pre-judging findings.

We have the utmost confidence in our members, who are all experienced professionals and are made aware of the communications guidelines from the outset. If an issue were to arise, it would be managed constructively and proportionately.

Membership is reviewed annually. Where a member feels that they are no longer able to meet the expectations of the group, they would be expected to step back.

Evaluation protocol paper overview

Policy context and purpose

- Australia introduced the Social Media Minimum Age Act in December 2025, creating a world-first restriction on social media access for under-16s.
- Around 1.2 million young people are expected to be affected through account deactivation or restricted access.
- The evaluation is designed to understand what impact this policy has in practice, not just whether it is implemented.
- The aim is to build a robust evidence base to inform future policy in Australia and internationally.

What the evaluation is trying to measure

- The study looks beyond compliance and focuses on real-world outcomes across five core areas:
    - Adherence to the policy, including awareness and circumvention
    - Digital behaviours and online experiences
    - Wellbeing, including psychological, social, and physical outcomes
    - Family dynamics, including parenting and relationships
    - Broader community attitudes and social norms
- It explicitly considers both intended and unintended effects, including potential harms and benefits.
- There is a strong focus on identifying differences across groups, including vulnerable cohorts such as Aboriginal and Torres Strait Islander communities.

Study design and methodology

- The evaluation uses a mixed-methods approach, combining quantitative and qualitative data.
- Sample size includes over 4,000 young people aged 10 to 16 and their parents or caregivers.
- Core components include:
    - Five waves of longitudinal surveys over two years
    - Passive smartphone tracking for behavioural insights
    - Linked administrative data such as health and education records
    - Interviews and focus groups capturing lived experience
- This combination allows the study to capture both what is changing and why it is changing.

Analytical approach

- The data will be analysed using both descriptive and advanced statistical methods.
- Longitudinal modelling techniques will examine changes over time, both within individuals and across groups.
- Causal inference will be supported through advanced methods such as Targeted Maximum Likelihood Estimation.
- Qualitative data will be analysed thematically to understand experiences, perceptions, and emerging patterns.
- Together, this ensures findings are rigorous, nuanced, and policy-relevant.

Focus on families and community

- The evaluation recognises that social media is not just an individual issue.
- It looks at impacts on:
    - Parenting practices and digital mediation
    - Family cohesion and shared activities
    - Community norms and attitudes toward youth social media use

- This allows a better understanding of how policy affects households and social systems, not just individuals.

Theory of Change and evaluation framework

- The evaluation is grounded in a Theory of Change, which maps expected short, medium, and long-term outcomes.
- This framework identifies:
    - How the policy is expected to work
    - What assumptions are being tested
    - Where unintended consequences may emerge
- The Theory of Change was developed through consultation with:
    - Academic experts
    - Practitioners
    - Young people and lived-experience groups
    - Internal stakeholders
- This ensures the evaluation is both evidence-based and grounded in real-world context.

Strengths of the study

- Uses multiple data sources, including surveys, behavioural data, and administrative records
- Tracks participants over time, allowing analysis of short, medium, and longer-term impacts
- Draws on validated measures where possible, increasing reliability
- Includes new measures tailored to the policy context
- Intentionally samples to improve representation, including Aboriginal and Torres Strait Islander communities

Limitations to acknowledge

- Attrition over five waves is expected and may reduce sample size over time
- Smaller sample sizes in later waves may limit statistical power
- As with all real-world policy evaluations, there are external factors that may influence outcomes

Ethics and governance

- Approved by the Australian Institute of Family Studies Human Research Ethics Committee
- Complies with the National Statement on Ethical Conduct in Human Research
- Adheres to the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander research
- Participation is fully consent-based and voluntary

Why this matters

- This is one of the first large-scale evaluations of a nationwide social media age restriction.
- Findings will:
    - Inform ongoing policy implementation in Australia & inform other governments
    - Contribute to global debates on youth digital safety

Q&A

Why can't this data be shared with the public?

Legal, ethical and governance constraints

- **Ethics obligations:** The study is **bound by Human Research Ethics Committee** approval, requiring confidentiality and use of data only for the approved evaluation purpose. Public release would breach these protocols.
- **Participant assurances:** Participants were **explicitly told their data would remain confidential** (unless legally required). Releasing it would break this commitment.
- **Controlled access:** Raw data is tightly restricted to authorised evaluators, academic partners and those named in the ethics approval.

Risk to data integrity and misuse

- **Misinterpretation and manipulation:** Public access could lead to data being misused, misinterpreted, or selectively analysed, producing misleading conclusions.
- **Undermines evaluation integrity:** Such misuse could damage the credibility and validity of the evaluation and its findings.
- **Loss of trust:** Any disclosure risk would **erode participant confidence** in eSafety and result in participants withdrawing

Privacy and re-identification risks

- **Re-identification potential:** Even without direct identifiers, combinations of demographic data could enable identification of individuals.
- **Highly sensitive content:** The dataset includes information on online harms, mental health and wellbeing, and vulnerable experiences, increasing risk of harm if exposed.

How are you managing privacy?

- **Privacy embedded end-to-end with expert oversight**: eSafety's Privacy Officer and Data Governance Lead were actively involved from procurement through to delivery, ensuring privacy considerations were built into every stage of the project lifecycle.
- **Strong contractual protections across all parties**: The **fieldwork provider Social Research Centre** and their **passive data collection subcontractor** are contractually bound under the Commonwealth MAS Panel Head Agreement to comply with the *Privacy Act 1988* and Australian Privacy Principles, with obligations flowing through to all subcontractors.
- **Engagement with specialised providers and privacy experts**: eSafety worked closely with the **fieldwork provider (including their privacy team)** and the **passive data provider** to review technical documentation, data handling processes and security arrangements before approval.
- **Trusted and accredited data linkage partner**: The **Australian Institute of Family Studies (AIFS)**—an **Accredited Integrating Authority and Accredited Data Service Provider**—supports data linkage under strict national governance frameworks set by the Office of the National Data Commissioner.
- **Rigorous ethics and consent processes**: The **Human Research Ethics Committee (AIFS HREC)** reviewed and approved the study, including the data management plan and all **participant and parent consent materials**, ensuring informed consent and appropriate handling of sensitive data.

- **High data security standards across providers**: Both the **fieldwork provider and passive data provider** meet recognised security standards (including ISO 20252 certification), and their systems and outputs were assessed to minimise risks of personal information exposure.
- **Ongoing monitoring and assurance**: Privacy risk is continuously assessed by eSafety, with a **Privacy Threshold Assessment (PTA)** already completed and provisions in place to undertake a **Privacy Impact Assessment (PIA)** if required as the project evolves.

Other relevant research

- **eSafety is maintaining a register** of other domestic and international studies examining the implementation and effectiveness of the Social Media Minimum Age. We welcome and encourage complementary research to help build the broader evidence base.
- **eSafety has also conducted a "pulse" survey** of parents to assess early compliance, with findings in a research report and reflected in its March compliance update, and we'll be looking to run these through out the year.
- Recent studies released by the **Molly Rose Foundation and the University of Chicago's Becker Friedman Institute for Economics** also make valuable contributions to the early evidence base.
- Findings from the **Molly Rose Foundation were broadly consistent** with eSafety's parent pulse survey and compliance insights. While interpretation may vary the data is similar.
- The University of Chicago study provides useful insights but its findings on compliance should be interpreted with caution due to how "non-compliance" was operationalised. The survey:
    - did not distinguish between social media use with or without an account
    - did not identify whether children held their own accounts on age-restricted platforms.
    - Despite these limitations, the study highlights important behavioural dynamics. Notably:
    - among children who continued to use social media, 52 per cent cited at least one social motivation, such as friends still using the platform
    - children were more likely to report recent use of age-restricted platforms where they believed a higher proportion of their close friends continued to use them.
- These findings underscore the importance of achieving a critical mass of behavioural change. Individual decisions are strongly shaped by peer norms. This reinforces the central role of platform compliance.

Freedom of Information requests, QoNs and Orders for the Production of Papers

Key topics covered in recent requests:

- Terms of Reference for the Academic Advisory Group and meeting minutes and agendas
- Correspondence between eSafety and the Lead Academic Partner and the Academic
- Advisory Group
- Correspondence between eSafety, the Minister's Office and/or the Department
- Data and privacy measures
- Documents submitted to Human Research Ethics Committee
- Access to the raw deidentified dataset
- Analysis power to detect impacts on particular groups of children, for example sexually diverse children
- Cost of the evaluation

Youth survey scrutiny

News media

Sky News August 3, 2025: 'It's Covid all over again': Labor bending at the knee to eSafety commissioner's advice on YouTube ban while turning blind eye to our freedom, education | Sky News Australia

Response

While children were less likely to say that their most recent experiences of grooming and bullying occurred on YouTube, compared to other platforms, it was the most reported platform where children had recently seen harmful content. In addition, even small percentages reported in the study represent thousands of children at a national scale.

Sky News July 11, 2025: 'It would be like banning a library': eSafety Commissioner 'misled' Australians on push to ban YouTube | Sky News Australia

Response

- **The research was published in line with standard publication timelines**, with the methodology report already publicly available. The research was not withheld to obscure findings.
- **Surveys are a well-established method in social science research,** and this study aligns with methodologies used to examine the digital lives of children, by respected institutions such as Pew Research Center, Common Sense Media, UNICEF Innocenti, and Ofcom. The Keeping Kids Safe Online survey was a rigorously designed empirical study grounded in best-practice research standards. **It was, developed in collaboration with domestic and international experts, informed by a taxonomy of online harms and the latest literature, subject to cognitive testing with children and parents to ensure clarity and sensitivity, and reviewed and approved by a formal ethics committee, ensuring it met high standards for research involving children.**
- **The survey focused on children's lived experiences, not platform mechanics.** However, the findings on exposure to harmful content, especially on platforms like YouTube and TikTok, underscores the need for further investigation into algorithmic amplification and content recommendation systems.
- While children were less likely to say that their most recent experiences of grooming and bullying occurred on YouTube, compared to other platforms, it was the most reported platform where children had recently seen harmful content. In addition, even small percentages reported in the study represent thousands of children at a national scale.
- **Self-reported data is a standard and valid approach in child-centred research**, especially when investigating subjective experiences like harm, bullying, or harassment. Children's voices are essential in understanding their digital lives, and their perspectives offer insights that cannot be captured through observation alone. Moreover, the report is transparent about its methodology and limitations, as is standard in ethical research

Education, Engagement & Awareness (EPAC & Comms)

Online Safety in Sport Summit (SIA)

This financial year we haven't paid anything yet, but we are due to pay:

- $50K for the eSafety Online Sport Summit held 19 May 2026 to Sport Integrity Australia.

We also pay $10k to Sport Integrity Australia under the Play By The Rules MOU.

eSafety/SIA Online Safety in Sport Summit

- Took place on Tuesday 19th May 2026 in the QT Hotel, Canberra.
- Jointly hosted by Sport Integrity Australia (SIA) and the eSafety, the Summit brought together senior leaders from sport, government, law enforcement, policy and the technology sector to strengthen collaboration and drive action on online abuse in sport.
- Attendees heard from speakers across the sector, including Dr Emma Kavanagh, a leading international researcher on online abuse from the University of Loughborough, as well as Australian athletes and officials with lived experience of online harms, and technology industry partners.
- eSafety agreed to contribute $50,000 towards costs e.g. venue hire, audio/visual equipment hire, collateral, catering.
- Formal agreement with SIA in place for the above arrangement, and SIA will invoice eSafety in June 2026.

eSafety/SIA MOU

This MOU will strengthen the national approach to online safety in sport through coordinated capability, support, and enforcement efforts by:

- Building **workforce capability** by delivering joint training, shared resources, and secondment opportunities across both agencies and the broader sport integrity network
- Providing **sector-wide support** by equipping staff, integrity managers, and sporting organisations with practical guidance on online safety and sport policy
- **Coordinating responses to emerging threats** through a formal process to identify and address online risks, including betting-related abuse and harms targeting women and girls
- Enhancing **collaboration and intelligence sharing** by enabling information exchange, co-designed education initiatives, partnerships with law enforcement, and cooperation on investigations to support safer online sporting environments.

Strat Comms

Awareness and reach - 1 July 2025 – 31 March 2026

More detail and disaggregated data is available in *0.9 Back Pocket Brief – eSafety Key Statistics*.

(Statistics are for eSafety.gov.au only. See *Key Statistics* for Be Connected)

Top lines

- 84% in website visitors (12m users per year, 1.3m per month), 12% increase in social media followers
- 44 media releases
- 30 external engagements
- **4 million Australians reached through our digital campaigns** – This includes 1.6m parents reached and 4,500 webinar registrations.
- Department campaign resulted in a 90% increase in overall page views on the website.
- Since **2020 16k educators trained in early years program** and **600+ staff trained in the tertiary sector**
- **Over 100k** people reached through our awareness & capability webinars and training this FYTD
- **70,000 young people reached in virtual classrooms**
- We have almost **1,500 eSafety champions** in schools across Australia (15% of schools)
- **Our Trusted eSafety Providers program have reached over 1.6m people**

Website	Almost **12M users** visited eSafety.gov.au since 1 July 2025 this financial year, an **84%** increase on the same period the year prior. This represents an average of 1.3M users to eSafety.gov.au each month this financial year to date. Although our website traffic is still strong, growth is starting to drop as more impact was felt from zero-click searches from Google's AI Overviews. This aligns with trends seen across websites generally. **eSafety resources** were downloaded over 225,000 times during this period. *Source: Google Analytics*
Email activity	**Almost 1.5M emails** (+1.459M) were sent from **143 email campaigns** in the second half of 2025, an 18% increase on the same period in 2024**.** **eSafety's subscribers grew 47%** this financial year to date (Jul 2025-Mar 2026), totalling **+90,000 subscribers** at March 2026. . *Source: MarComms reporting - per Monthly MO Reports*
Media stats	eSafety issued **44 media releases** and statements and received **over 22,000 media mentions** this financial year to date. *Source: Isentia Reporting*
Social media stats	eSafety's **social media following** grew 12% across the second half of 2025 to **95,000 followers.** **331 social media posts** were published in the second half of 2025. These received **2.6 million impressions**, a **174% increase** on the same period in 2024. *Source: MarComms reporting - per Monthly MO Reports*
Events delivered	The Commissioner delivered more than **30 external engagements, reaching an estimated 5,000 attendees (in-person and online).** *Source: JIRA Commissioner Engagement Reporting*
Digital campaigns	Across the second half of 2025, eSafety reached **close to 4 million Australians** through targeted digital campaigns, driving **more than 190,000 users** to trusted safety information and support.

<table>
<tr><td></td><td>This included 1.6 million reach to parents and carers, generating 4,500+ webinar registrations, and tens of thousands of young people accessing help on tech based abuse and coercive control.</td></tr>
<tr><td>SMMA Campaign Impacts</td><td>

The campaign has been active since mid-October 2025, and ended in April 2026.
eSafety worked with the Department to better understand information needs and/ or information gaps.
This informed our content and resource development, and helped us tailor new and updated resources to support parents, carers and educators in understanding, and being prepared for the social media age restrictions.
This content was published to eSafety's Social Media Age Restrictions Hub, and included frequently asked questions, get ready guides and fact sheets, as well as video content.
While the Department is best placed to speak to evaluation of the campaign, the data available to us suggests a considerable impact.
It delivered a significant lift in overall website traffic to eSafety.gov.au in the opening months of the campaign. There was around 90% increase in overall page views, for the period of October 2025 to January 2026 (compared to the same period the year prior).
If asked about the exact numbers in the QoN from December – (SQ25-002581) Figures looking at overall users to eSafety.gov.au (rather than the social media hub page) more accurately reflect the uplift we saw from the Department's public information campaign because the call to action in the campaign encourages people to visit our main landing page, eSafety.gov.au. When we refer to figures for the Social Media Age Restrictions Hub, this is a subset of pages relating to the campaign-specific page.

Data noted below, as at 1 May -
<table>
<tr><th>Total website traffic</th><th>From 1 October 2025 to 31 March 2026</th><th>YoY % change</th></tr>
<tr><td>Total users</td><td>8.0M</td><td>48.4%</td></tr>
<tr><td>Page views</td><td>12.2M</td><td>46.8%</td></tr>
</table>

</td></tr>
</table>

- The June 2023 notice on AusTender referred to an Approach to Marketing to spend $66k on an eSafety awareness initiative. It referenced research from 2022 indicating that public awareness of eSafety was at **22%**.
- The resulting awareness initiative was the 'Your eSafety kit' general awareness campaign. Phase 1 of the campaign went to market between 23 Oct and 3 Dec 2023, and phase 2 was in market between 4 Sep to 16 Oct 2024 (used to promote the resources from the Family Capacity Building project).
- eSafety research conducted in 2025 measured prompted awareness of eSafety at **38%**.
- The campaign exceeded all targets, and public awareness increased. It's difficult to attribute the increase in awareness directly to the campaign. eSafety research indicates that people become first aware of eSafety through a range of channels, including news media stories, word of mouth, their own internet research, and advertising.
- eSafety's education and awareness initiatives aim to strengthen the Australian public's understanding of online harms, promote protective behaviours for individuals and families in online spaces, and empower people to seek help and support and take appropriate action when needed.

Education, Prevention and Communities

Key talking points

How we engage

- We take a **whole-of-life approach**, from early years through to older Australians.
- We combine **direct engagement (youth, parents, educators)** with **trusted partnerships** (schools, community organisations, peak bodies).
- Programs are **inclusive, accessible and culturally relevant**, reaching diverse and priority communities.
- We scale impact through **national training, digital delivery and partner networks**.

Why it matters

- Online harms are **growing and evolving (especially with AI)** and affect different groups differently.
- **Prevention works best when reinforced across families, schools and communities**.
- Partnering with trusted organisations helps us **reach more people and build credibility**.
- This coordinated approach builds **national capability**, leading to safer and more inclusive online experiences for all Australians.

Children & Young People

- We directly engage young people so their **lived experience informs online safety policy and programs**.
- The **Youth Council received 575 applications this year**, showing strong engagement and awareness.
- Our **Mighty Heroes program** continues to build early digital literacy through interactive tools for ages 5–8, driving strong engagement with children and families.

Parents & Carers

- Our **Parent Advisory Group includes 12 national organisations** representing diverse communities across Australia.
- It helps us **test resources, strengthen messaging, and reach priority groups**, including culturally diverse, regional and vulnerable families.
- Ensures our advice is **practical, inclusive and grounded in real family experiences**.

Family Capacity Building

- Focused on **prevention and early intervention**, supporting parents to talk regularly with children about online safety.
- Delivered **multilingual resources, a national campaign, and 9,000+ family books**.
- Expanding support for **families of children with disability and neurodivergence**.

Early Years

- Since 2020: **43,000+ books distributed and 16,000+ educators trained**.
- Updated resources following **2025 legislative changes**.
- Ongoing engagement supports **safe online habits from the earliest years**.

Schools

- **NOSEC includes 60 members** across all school sectors nationally.
- **1,467 eSafety Champions** now active, covering about **15% of Australia's ~9,600 schools**.
- Goal is **nationwide school-level capability**.

Awareness & Capability

- Reached **99,000+ people (FY25/26 YTD)** through training and sessions.
- Delivered **Virtual Classrooms to 70,000+ students** on practical online safety skills.
- Training covers emerging risks including **AI harms, deepfakes, cyberbullying and coercive control**.
- Expanding into **frontline sectors** (local government, libraries, DFV services, residential care).
- Provides tailored **"social media self-defence" training** for high-risk groups.
- Focused on **building practical skills and national capability at scale**.

Trusted Providers

- **25 accredited providers** delivering quality, curriculum-aligned education.
- Reached **1.6M+ people in 2024–25**, including:
    - **1.37M students**
    - **53K educators**
- Key model for **scaling national reach through partnerships**.

Tertiary Sector

- Engagement with **every Australian university**.
- **600+ staff trained** and growing engagement (1,500+ subscribers).
- Provides tools to support **safe digital environments on campus**.

Women & Online Safety

- Focus on **preventing technology-facilitated gender-based violence**.
- Backed by a **$10M grants program (2023–2028)** supporting prevention and behaviour change.

Sport

- **Sport Hub** provides practical tools for **players, parents, coaches and officials**.
- Supports prevention and response to **online abuse in community sport**.

Digital Literacy (All Ages)

- **Whole-of-life approach** to digital safety.
- **Mighty Heroes** driving strong early engagement.
- **Be Connected has supported ~3 million older Australians** via **3,800+ community partners**.

Detail

Children and Young People

- The Children, Youth and Families (CYF) team leads eSafety's work to engage directly with children and young people, ensuring their perspectives and experiences help inform online safety approaches.
- CYF focuses on reach, engagement and participation, using child- and youth-friendly platforms and formats to connect with young Australians where they are online.
- A key mechanism for youth engagement is eSafety's **Youth Council**, which provides consultative insights from young people on emerging online issues and lived experience.
- Interest in the Youth Council remains exceptionally strong, with **575 applications** received this year, demonstrating high levels of youth awareness and willingness to engage on online safety issues.
- CYF also delivers eSafety's flagship Mighty Heroes digital literacy products for younger children, including interactive games that introduce core online safety concepts in age-appropriate, engaging ways.
- Recent Mighty Heroes initiatives continue to drive strong engagement with children and families, supporting positive online behaviours from an early age.

Parents/carers

- eSafety convened its Parent Advisory Group (PAG) in **November 2025**
- The PAG is not a group of individual parents; it comprises **12 nationally recognised organisations** that work directly with parents and carers across Australia and represent diverse family and community perspectives.
- Member organisations reflect a broad cross section of Australian communities, including **Culturally and Linguistically Diverse families, First Nations peoples, regional and remote communities, people with disability, LGBTIQ+ communities, and families from low socio-economic backgrounds**.
- PAG members support eSafety to:
    - **Inform and strengthen parent and carer messaging,** including guidance related to the SMMA and broader online safety priorities.
    - **Review and test parent facing resources**, including the redevelopment of eSafety's **Online Safety Parent Guide**.
    - **Assist with network building and dissemination of resources** to reach hard to engage and priority communities.
- The PAG complements broader consultation activities and supports eSafety's commitment to working with trusted organisations that engage families every day.

Organisation	Representatives (Primary, Secondary)
• Australian Childhood Foundation	• Kelly Royds, Dr. Cyra Fernandes
• Beyond Blue	• Carly Crawford, Jessica James
• Body Safety Australia	• Deanne Carson, Jay Jones
• Bravehearts	• Kate McGill, Lauren Adams
• Ctrl+Shft	• Maggie Dent, Madeleine West
• Deakin University	• Dr. Xinyu (Andy) Zhao, Luci Pangrazio
• Next Level Collaboration	• Jess Rowlings, A/Professor Matthew Harrison
• ReachOut	• Ben Bartlett, Fiona Tuttlebee
• Triple P International	• Carol Markie-Dadds, Eva Meester
• University of Sydney	• Dr. Raffaele Fabio Ciriello
• UQ Parenting & Family Support Centre	• Professor Matthew Sanders
• Yourtown	• Kimberley Harper

Family Capacity Building

- This work is **NPP funded through the *National Strategy to Prevent and Respond to Child Sexual Abuse***.
- eSafety delivers targeted family capacity-building initiatives to support parents and carers to recognise and prevent harmful online behaviours, including online child sexual abuse. The focus is on prevention, supporting parents and carers to have regular, age-appropriate conversations with children about online safety.
- The first **tranche of resources was released in September 2024**, including animated videos and practical guidance for families, also translated in multiple languages.
- Key outputs include a national parent and carer awareness campaign, the *Let's Talk About Being Safe Online* family book (9,000+ hardcopies distributed), and a resource hub for child and family sector professionals.
- Upcoming work focuses on new resources to support families of children with neurodivergence and disability (released later this year).

Early Years

- The eSafety Early Years Program was launched in 2020 to support educators, families and young children to build awareness of online safety in the early years.
- Since launch, the program has achieved strong engagement, with more than 43,000 copies of the *Swoosh and Glide* books distributed to families and early childhood education and care services, and over 16,000 educators completing eSafety's online professional learning modules.
- Following the introduction of new legislation relating to digital technologies and devices from September 2025, eSafety has updated its Early Years website and resources and delivered targeted engagement to the sector.
- To date (April 2026), eSafety has hosted three webinars reaching approximately 1,600 educators and has shared tailored guidance through newsletters, social media channels and industry stakeholders.
- Ongoing provision of current, relevant and accessible information remains critical to supporting the sector and Australia's youngest children to develop safe and positive online habits now and into the future.

Schools/NOSEC

- The National Online Safety Education Council (NOSEC) was established by the eSafety Commissioner in December 2022.
- NOSEC is a key stakeholder group, meeting with eSafety 4 times per year (once per school term) to exchange online safety insights and updates. NOSEC members also serve as crucial touchpoints during critical online safety incidents in schools.
- Currently (April 2026) there are 60 Council members representing each of the Government, Catholic and Independent school sectors in every Australian state and territory.

eSafety Champions

- The eSafety Champions Network comprises school staff who make online safety a priority in their schools.
- The goal of the program is to resource school staff with knowledge, skills and tools to build online safety capacity in their school communities.
- eSafety aims to have an eSafety Champion in every primary and secondary school. There are 1,467 school-based staff currently registered as eSafety Champions (eSafety, April 2026), representing approximately 15% of the 9,673 schools in Australia (ABS, 2026).

Awareness and Capability

- eSafety's Awareness and Capability team provides coordination, design and delivery of eSafety training to key audiences across Australia. In the 25/26 financial year, the team has presented to over 99,256 people (to 31 March 2026).
- Our professional learning for **educators and youth-serving professionals**, and awareness sessions for **parents and carers**, cover a range of topics that focus on the latest online safety trends and issues, research, case studies and prevention and support strategies. In 2025-2026, our new offerings include:
  - Recognising online coercive control in young people's lives
  - The changing face of cyberbullying
  - AI assisted image-based abuse: Navigating the deepfake threat
  - Understanding and using parental controls to help protect your child online
  - Navigating screen time: tools for today's families
  - Exploring the online experiences of boys and young men
  - The trust trap: navigating friendships, pressure and manipulation online
  - How AI is influencing new online risks for children and young people
  - Risks and rewards of online communities: What educators and youth-serving professionals need to know
  - Influencers, ideology and impact: How algorithms influence and reinforce harmful beliefs
- During key dates such as Safer Internet Day, Bullying No Way - National Week of Action and Child Protection Week, we provide opportunities for **primary students across Australia** to participate in live online Virtual Classrooms. The sessions cover a range of current online safety issues for students from Years 3-6, such as safer gaming, online chat safety and using safety skills for protection online. We have reached over 70,000 students so far this financial year.
- The team also offers customised '**Social media self-defence**' training for high-profile individuals and organisations – including current and aspiring politicians, journalists, school leaders, researchers and technologists, and elite athletes – focusing on social media safety, abuse prevention, and wellbeing strategies.
  This year we have scheduled 2 specific nation-wide sessions for the local government sector, targeting those working for local councils and local government elected and aspiring leaders.
- In 2026 we are scaling our efforts to reach frontline workers via **sector-wide webinars** for audiences including library staff, practitioners working with children and young-people in the residential care sector; domestic, family and sexual violence frontline workers; early years sector leaders and

educators; and we continue to offer sessions for key tertiary sector stakeholders and training for sporting organisations and clubs.

Trusted eSafety Providers

- The Trusted eSafety Provider (TeP) program, established in December 2019, supports schools and community organisations around Australia to access high-quality online safety education delivered by external providers, and raise awareness of eSafety's regulatory and reporting schemes.
- Endorsed providers must demonstrate suitable expertise and experience, evidence-based and curriculum-aligned programs, and compliance with child safety and insurance requirements.
- eSafety works with providers through a collaborative community of practice to share research and insights, and to promote ongoing professional development.
- As of April 2026, there are 25 providers participating in the program.
- In the 2024-2025 annual reporting period, endorsed providers reached a total audience of 1,625,668 including:
  - 1,374,726 students
  - 53,092 educators
  - 34,400 parents
  - 162,640 individuals in non-school settings

Tertiary Sector

- eSafety supports the tertiary sector (universities, TAFES and private colleges) to create safer online environments for all those studying and working in these institutions.
- The Tertiary Hub on the eSafety website has resources to support students, staff and institutions, including the Tertiary Toolkit comprised of 12 resources on topics including safe social media use and guidance for responding to critical incidents.
- Outreach with the sector has engaged staff from over 50 different tertiary organisations, including every university in Australia. Over the past 12 months:
  - the audience for the Tertiary Electronic Direct Mail (EDM) has grown from 75 to 1,521 subscribers.
  - 605 tertiary staff have attended an eSafety staff training or information session.

Women

- eSafety provides information, practical resources and training to the general community, frontline workers, business and other key stakeholders to prevent and respond to technology-facilitated gender-based violence and to promote safe, inclusive and gender equal online spaces.

- eSafety delivers the Preventing Tech-based Abuse of Women Grants Program which aims to improve the safety of Australian women and their children through the prevention of technology-facilitated gender-based violence. The program supports projects that target people who perpetrate technology-facilitated abuse and/or change attitudes and behaviours in the broader community, as well as projects that specifically target women and children. A total of $10 million in grant funding has been made available provided from 2023 to 2028 across three rounds.

Sport

- eSafety's Sport Hub is a one-stop-shop for administrators, coaches, officials, parents and competitors to learn ways to prevent and manage online abuse in community sport.
- It includes practical information on how to recognise online abuse, how to deal with online abuse, eight ways to stay safe online and promotional resources for clubs to download and show their support.
- It also includes tailored advice and scenarios for sports administrators, coaches and officials, athletes and competitors and sport parents.

Digital literacy

- The Mighty Heroes program is eSafety's flagship digital literacy program for low- mid primary school students. The program features animated Australian bush animals (Wanda, River, Dusty, Billie) designed to teach children aged 5-8 about online safety. In its first weeks a new Mighty Heroes Game – Robo Raven and the Ancient Relics – drove a 48% increase in traffic to eSafety's educator pages (Google Analytics report March 2026).
- eSafety co-delivers the Be Connected program alongside the Department for Social Services and Good Things Australia. The program is designed specifically to support people aged 50 and over to participate confidently in the digital world. It offers free, plain-language online learning alongside face-to-face, community-based support, recognising different learning styles and paces. The program has supported nearly 3 million older Australians through more than 3,800 community partners delivering local training across Australia.

Engagement with the mental health sector

- eSafety has ongoing engagement with the mental health sector, both through regular meetings and in response to critical issues. This allows us to share information on emerging online harms and how they are impacting young people, schools and families.
- For example, through the introduction of the Social Media Minimum Age changes we consulted regularly with key mental health organisations including Kids Helpline, Beyond Blue and Headspace on content development and referral pathways. This meant we could be confident our messages to young people and families dealing with the changes were aligned, and also that people could quickly access help and support.
- We also deliver training on emerging online safety issues to the broader mental health sector. Between July 2025 and April 2026, we provided targeted professional learning to over 1,400 staff from key organisations —including Lifeline, headspace, Neami National, Yourtown, the Australian Counselling Association, and multiple state health and education departments. These sessions covered essential topics relevant to the mental health and safety of children and young people, such as recognising online coercive control, responding to tech-facilitated abuse, preventing child sexual abuse online, addressing AI-assisted image-based abuse and deepfakes, and supporting help-seekers experiencing online harms.
- During this period, notable engagements included a webinar for 216 members of the Australian Counselling Association on recognising coercive control in young people's lives, a headspace national education briefing for 115 people, and a large-scale session on the online experiences of children and young people to over 400 members of WA Child and Adolescent Health Services.

Deep fakes in schools

- eSafety supports schools to prepare and respond to online safety issues, including AI generated deepfakes.
- The Toolkit for Schools includes a module added in June 2025 to address the increasing prevalence of deepfakes - Respond 3B – Guide to responding to image-based abuse involving AI deepfakes.
- We have raised awareness of this issue by publishing a range of advisories and guidance, including the 'Deepfake damage in schools' online safety advisory and a media release urging schools to report deepfakes in June 2025, delivering professional learning webinars on AI deepfakes throughout 2025, and highlighting the issue through our regular Education newsletter.
- eSafety has advocated on this issue across Government, including the eSafety Commissioner addressing the 17 October 2025 Education Ministers Meeting and writing to Education Ministers in December 2025. We have also prioritised this topic in meetings of the National Online Safety Education Council (NOSEC) that includes representatives from Government, Catholic and Independent school sectors in every State and Territory.

- Finally, eSafety provides direct support to school sectors on an ad-hoc basis when we become aware of issues (e.g., through media reporting) or when we are contacted directly by schools. This involves providing guidance on relevant reporting options, sharing eSafety education resources, and linking to support services that can assist impacted individuals.

How do we reach vulnerable communities?

- eSafety co-designs our resources with vulnerable communities e.g. co-design with Aboriginal and Torres Strait Islander organisations, LGBTIQ+ groups, CALD communities and people with disability to ensure materials reflect their lived experience, cultural context and real online risks.
- We undertake extensive community consultation (e.g. workshops, roundtables and partnerships with community organisations) to shape content, delivery methods and messaging so they are accessible, culturally safe and relevant.
- We partner with frontline and community-led organisations to test and refine resources, ensuring they are practical for those supporting vulnerable audiences.
- We incorporate feedback from stakeholders and those who engage with our resources to continuously improve resources to better meet their needs.

Preventing Tech-based Abuse of Women Grants Program – Funded Projects:

ROUND 1	
Organisation	**Project**
Global Institute for Women's Leadership **State: ACT** **Funding: $494,610**	This project aims to develop an evidence-based, intersectional approach to the prevention of tech-based abuse of women. The project will develop digital resources and a communication platform underpinned by a prevention framework addressing the drivers of tech-based violence.
Gippsland Women's Health **State: VIC** **Funding: $493,486**	This project aims to engage rural women in a co-design prevention of violence program. The project will facilitate rural consultation and workshops to develop digital resources and a prevention-based communication strategy that addresses the drivers of tech-based abuse and improve women's safety.
Settlement Services International Limited **State: NSW** **Funding: $488,471**	This project aims to enhance the understanding of online safety and tech-based abuse in relation to domestic family violence through co-designing resources relevant to CALD women and children.
Monash University **State: VIC** **Funding: $444,450**	The project aims to help the domestic family violence service system, researchers and women to understand how abusive partners may be monitoring or following people using technology and provide education on monitoring prevention. The project will develop evidence-informed resources for the perpetrator intervention sector in urban and non-urban locations, which can be rolled out across Australia.
Centre for Cyber Resilience and Trust (Deakin University) **State: VIC** **Funding: $340,562**	This project aims to reduce technology-facilitated abuse by engaging with perpetrators through digitally targeted advertising and search engine optimisation techniques, intervening at the research stage of those contemplating technology-facilitated abuse.
University of Melbourne **State: VIC** **Funding: $243,000**	This project aims to develop an anti-online harassment software co-designed with girls and young women. Through participatory action research, natural language processing, generative artificial intelligence (AI), and machine learning, the software will act as an 'upstander' against online abuse in real time.

ROUND 2	
Organisation	**Project**
Museum of Sticks & Stones **State: QLD** **Funding: $374,000**	This project aims to reduce the normalisation of misogynistic ideologies and their harmful impacts by seeking to understand and address the root causes driving young men (aged 15–25) toward these beliefs. The project combines research, community education and co-design with young men to create a documentary series.
Multicultural Families Organisation Inc. **State: QLD** **Funding: $355,000**	This project aims to educate potential perpetrators from culturally diverse backgrounds that tech-based abuse is a serious offence and educate them on the effect their abuse has on the victims and to change their behaviour. It has a cross-community approach that includes educational workshops, multilanguage resources, a social media campaign and resources for parents.
Queensland Remote Aboriginal Media Corp. (First Nations priority funding project) **State: QLD** **Funding: $206,000**	This project will aim to develop a range of relatable, culturally relevant and engaging resources co-designed with communities to prevent tech-based abuse against First Nations women in regional and remote QLD
Katherine West Health Board Aboriginal Corp. (First Nations priority funding project) **State: NT** **Funding: $394,000**	The project aims to reduce tech-based abuse against women and children by engaging First Nations men, particularly those at risk of perpetrating, in the co-design of targeted initiatives including community led programs and culturally tailored resources address the underlying drivers of tech-based abuse.
The University of Western Australia **State: WA** **Funding: $369,000**	The project aims to develop effective co-designed resources and educational content for regional primary industry-based communities in WA including farming, mining/energy and fisheries, guided by the voice of boys and young men.
La Trobe University **State: VIC** **Funding: $374,000**	This project aims to expand the evidence base on transgender women's experiences of tech-based abuse and develop evidence-informed, community-led primary prevention resources. These resources will engage cisgender men who perpetrate tech-based abuse and address its underlying drivers.
Jesuit Social Services **State: VIC** **Funding: $369,000**	The project aims to understand the nature and drivers of tech-facilitated stalking behaviours within dating and intimate partner relationships among 16–24-year-olds. The project will generate new knowledge about the dimensions and causes of abusive behaviours among young people in dating and intimate partner relationships.
Royal Melbourne Institute of Technology **State: VIC** **Funding: $371,000**	This project aims to examine gaming influencer content and gender norms. By exploring gaming influencer content as a potential site of gender socialisation, the project will generate an understanding of what gendered meanings are communicated through gaming influencers and the impact of this on the gendered worldviews and development of tween boys.

The Flagstaff Group **State: NSW** **Funding: $314,000**	The project aims to support women with disability in recognising, preventing, and responding to tech-based abuse through engaging and inclusive offline games and a national awareness campaign. The project outputs will address the drivers of tech-based abuse of women with disabilities and support shifts in social norms that contribute to tech-based abuse.
ACON Health Limited **State: NSW** **Funding: $374,000**	The project aims to address the drivers of tech-based abuse against LGBTQ+ people, with a particular focus on First Nations LGBTQ+ people, and improve LGBTQ+ community safety through building community capacity to prevent tech-based abuse.

Grants summary

eSafety Grants Administration and Assessment Framework

The **2022 ACMA Audit Report** confirmed that eSafety delivers its grants in line with recognised best practice.

Grant applications are evaluated by an **assessment committee of 10 members**, including **five external representatives**. The **Chair** is responsible for ensuring that recommended projects are appropriately identified and have achieved strong results against the defined assessment criteria.

Assessment Criteria

Applications are assessed against the following key criteria:

- **Eligibility**
    - The applicant must be an Australian organisation registered with the **Australian Charities and Not-for-profits Commission (ACNC)**.
- **Organisational Capacity and Capability**
    - Demonstrated knowledge, skills, and experience of the individuals responsible for delivering the project.
- **Project Need**
    - A clear rationale for why the project is required, supported by relevant evidence. This may include:
        - Service delivery data
        - Stakeholder feedback
        - Previous project evaluations
        - Published research
        - Relevant plans and frameworks
- **Impact and Sustainability**
    - The potential for the project to be sustained beyond the grant period
    - Ability for the project to be scaled or replicated across different locations or target groups

Portfolio Considerations

In addition to merit-based assessment, the panel seeks to ensure that funded projects:

- Provide benefits to a **diverse range of community cohorts**
- Are delivered across a **broad geographical and jurisdictional spread**
- Represent a **wide range of organisation types**

Governance and Best Practice Principles

The **Commonwealth Grants Rules and Principles (CGRP)** provide guidance on best practice grant administration, including merit-based and competitive processes.

These principles underpin eSafety's grant assessment framework, ensuring that each funding round is conducted in a:

- **Transparent**
- **Defensible**
- **Equitable**
- **Outcomes-driven**

manner that supports sound decision-making and demonstrates **value for money**.

eSafety also recognises the complexity of facilitating panel discussions and ensures that deliberations are carefully guided to achieve fair, balanced, and evidence-based funding recommendations.

Gov & Business Ops

General Enquiries

General talking points

- The eSafety Commissioner has seen a steady increase in the number of public enquiries received since its inception in 2015.
- The introduction of the Social Media Minimum Age requirements and the associated public campaigns generated a significant further increase. eSafety has received over 1,800 enquiries related to the SMMA requirements since June 2025.
- The total number of enquiries received through the contact-us form on the eSafety webpage:

Year	No. of enquiries
2026 (up to 30/04/2026)	2,549
2025	6,276
2024	4,140
2023	3,446
2022	3,076

TFA Service

Key points

- **Extended funding:** The TFA Service has secured **$5.4 million for an additional 12 months**, extending operations through **June 2027**.
- **Core purpose:** It aims to **raise awareness of tech-facilitated abuse in domestic, family and sexual violence (TFA-DFSV)** and build frontline workers' capability to **recognise, respond, and manage risks in digital contexts**.
- **Service delivery model:** Support is provided via a **dedicated phone line** and an **online hub**, offering tailored advice and resources for both frontline workers and victim-survivors.
- **Strong and growing demand:** Since October 2024, the service has handled **600+ enquiries**, with significant engagement from frontline workers, and **20,000+ resource views**, highlighting widespread need.
- **Impact and future direction:** Early evaluation shows **positive impact and trust**, with key future priorities including **enhanced training and sector capability-building**, ahead of a final report due **June 2026**.

General talking points

- TFA has been allocated **$5.4 million in funding for a further 12-month period**, extending through to June 2027. Questions about funding are most appropriately directed to the Department.
- The purpose of the Service is to increase awareness of TFA-DSFV and support frontline workers to better recognise, respond and apply their risk assessment and safety planning expertise to online and digital environments.
- The Service provides support through operation of a dedicated phone service for frontline workers, complemented by an online TFA support hub, including resources for both frontline workers and victim-survivors.
- We are a trusted source of guidance, with extensive experience supporting frontline workers seeking assistance and connecting help seekers with appropriate services to ensure they receive the support they need.

- Since the establishment of the Service in **October 2024, eSafety has received more than 600** enquiries from frontline workers and help seekers relating to TFA-DFSV, across both phone and online web channels.
- **Almost half of these enquiries (approximately 275) have come from domestic, family and sexual violence services and other frontline workers across Australia.**
- **Concerns about monitoring and tracking** of a client represent the majority of contacts from frontline workers, followed by requests for education and training to recognise TFA and enhance their ability to support clients effectively.
- **Our TFA-DFSV online resources have also been viewed more than 20,000 times**, demonstrating strong and growing demand for information and support.
- **An independent evaluation of the Service is currently underway.** Final report expected June 2026 and will incorporate direct feedback from DFSV service providers, the sector, and frontline workers.
- Early evaluation insights highlight:
    - positive impact of our resources, tailored advice, support channels and technology knowledge expertise.
    - identification of priority focus areas for ongoing and future service delivery including sector training and capability support.

Note: Late 2025, some media articles incorrectly reported 20,000 contacts to the service, confusing the website views figure provided (over 20,000) with the service contacts figure (over 400).

OSA Review

General talking points and Government response

- The Online Safety Act Review was an independent statutory review. The Government has released its response to the review, which confirms that the Government intends to implement, or further consider, **64 of the 67 recommendations**. It also which the Government has stated is its highest priority is to legislate a digital duty of care.
- eSafety welcomes the Government's response, which builds upon the review report that positively affirmed eSafety's role and identified ways to strengthen our powers and ability to keep Australians safer online.
- Questions about the Review and the Government's response are most appropriately directed to the Department.
- We continue to work with the Department and Government as it progresses reform related to the Review.

Note: Questions about the progress or implementation of specific recommendations in the Review should be directed to the Department.

Questions about the status of the duty of care

- The Government is developing draft legislation to implement a Duty of Care in Australia under the Online Safety Act.
- Questions about the status of the duty of care are best directed to the Department.

Questions about industry obligations or what harms will be covered under the duty of care

- Questions about the design of the duty, including industry obligations of care or what harms will be covered, are best directed to the Department.
- We will continue to work with the Department and Government to progress the duty of care.

Questions about the online hate recommendations in the Review

- Whether specific recommendations of the Review are taken up is a matter for the Government.
- However, eSafety can note the Government has committed to introducing a duty of care under the Online Safety Act.
- eSafety will continue to work with the Department, Government and other key stakeholders, including the Special Envoy to Combat Antisemitism to progress reform to address online hate, including antisemitism, under the Online Safety Act.

Note: *Further talking points on online hate are available in Key Issues Brief – Online hate, including antisemitism.*

Questions about the adult cyber abuse scheme threshold under the Review

- The Review acknowledged the importance of our complaint schemes. We anticipate that our complaint schemes will continue to operate and complement the duty of care.
- Whether specific recommendations of the Review are taken up is a matter for the Government and any subsequent legislation is a matter for the Parliament.

If pressed on duty of care:

- While the design and model for the duty of care are a matter for the Government and questions are best directed to the Department, we note what the Government has stated in its response:
  - The duty of care will place obligations on service providers to proactively and effectively manage the risk of harms from the use and misuse of their platforms and services.
  - The duty of care will support broad, risk-based and proportionate regulation of all digital service providers.
  - The duty of care will provide a legislative framework that can better accommodate changes in technology and services.

eSafety submissions to inquiries

Date	Inquiry title	Recipient / Organisation
January 2025	Inquiry into the impacts of harmful pornography on mental, emotional and physical health	New South Wales Standing Committee on Social Issues.
June 2025	Anti-Bullying Rapid Review	Australian Department of Education
July 2025	Review into the System Responses to Child Sexual Abuse	Queensland Child Death Review Board
August 2025	Capability of law enforcement to respond to cybercrime [*Invited to lodge additional evidence following 2023 submission]*	Parliamentary Joint Committee on Law Enforcement
September 2025	Harnessing Data and Digital Technology	Productivity Commission
September 2025	Harnessing Data and Digital Technology [*DP-REG Joint Submission*]	Productivity Commission
September 2025	Internet Search Engine Services Online Safety Code	Senate Environment and Communications References Committee.
September 2025	Criminal Code Amendment (Post and Boast Offence) Bill 2025	WA Standing Committee on Legislation
May 2026	Inquiry into racism, hate and violence directed at Aboriginal and Torres Strait Islander people	Joint Standing Committee on Aboriginal and Torres Strait Islander Affairs
(Intended) 29 May 2026	Update to Modernise and Harmonise the Classification Guidelines 2025	Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

Age Assurance

Age Assurance Technology Trial

- The Australian Government provided $6.5 million to conduct an Age Assurance Technology Trial (2024–2025). The findings from the trial are one of several inputs we considered when developing regulatory guidance for the Social Media Minimum Age, as well as in the implementation of other regulatory schemes.

- The trial was not a ranking or approval exercise – eSafety does not expect that platforms must use the technologies included in the trial, and use of those technologies will not necessarily mean platforms are compliant.

    - The results of the trial do **not tell** us or industry exactly what technologies they must use, nor is it a certification process for approving technologies for use.
    - The **report does not endorse certain types of technology**, nor does it determine whether age assurance technology should be implemented or mandated in specific contexts.

- **Ongoing engagement:** The trial project is now complete. Since then, eSafety has had contact with Age Check Certification Scheme (ACCS), one of the organisations involved in the trial, in their capacity as a certification and accreditation body, where they have shared updates as relevant international standards have been published.

    - eSafety virtually attended (and purchased a ticket) to the 2026 Global Age Assurance Standards Summit, hosted by ACCS, to understand developments in the age assurance industry.

Age Assurance Technology – Accuracy and bias concerns

- We are aware of ongoing concerns about the accuracy of certain technologies, and in particular the use of facial age estimation for younger users close to the threshold age of 16. This is a known and expected finding.

- No method is 100% effective – and eSafety has often said that age assurance plays a role but is **not a silver bullet** for online safety issues. eSafety's regulatory guidance sets out our expectations regarding reasonable steps, including that platforms should take a **layered or 'waterfall' approach** across the user journey, combining measures to build cumulative confidence in a user's age.
- Age assurance is also only one element for platforms taking reasonable steps. eSafety is also examining all the practices of a platform – including the messaging they provide to users and effective measures for reporting underage accounts.
- ***Note:*** *Further talking points on preliminary enforcement action are available in KIB – SMMA – Compliance.*

Testing

- The US National Institute of Standards and Technology is conducting ongoing testing and evaluation of **facial age estimation technology**. Since testing began, they have expanded to report on results specifically for ages 13-16.

    - Testing is ongoing, and eSafety is monitoring results, among other sources of information, to assist us in understanding how this technology is continuing to evolve.
    - Results were last updated in **May 2026**, evaluation results for over 40 algorithms have been published since testing started in 2024.

- Providers can resubmit algorithms, allowing the testing to demonstrate improvements in metrics like the Mean Absolute Error. However, different algorithms perform differently on different cohorts, making generalised reflections challenging.
- These results demonstrate that the technologies are quickly evolving – however, they still need to be evaluated in their implementation contexts, not just testing environments.

Standards

- Descriptions and status information of select relevant international standards relating to age assurance are included below:

Standard	Description	Status
ISO/IEC 27566-1:2025, Information security, cybersecurity and privacy protection – age assurance systems – Part 1: Framework	This document establishes a framework for age assurance systems and describes their core characteristics, including privacy and security, for enabling age-related eligibility decisions.	**Published in December 2025.** The Standard has been made available by the ISO for **free.** ACCS (UK-based Age Check Certification Scheme) is offering certification against this standard.
IEEE 2089.1-2024 IEEE Standard for Online Age Verification	Framework for the design, specification, evaluation, and deployment of online age verification systems are established in this standard. This standard provides practical implementation information. This standard is the second in a family of standards focused on the 5Rights principles (see below)	**Published May 2024** ACCS (UK-based Age Check Certification Scheme) is offering certification against this standard.
IEEE 2089-2021 Standard for Age-Appropriate Digital Service Framework	Establishes processes by which organisations seek to make their services age-appropriate. Doesn't provide technical guidance regarding age assurance.	**Published 2021**

The Australian **Age Assurance Technology Trial (AATT)** did not test just a small set of vendors—it evaluated a **large, diverse field of providers**:

- **~48 vendors (over 60 technologies)** in the final report
- **Over 50 participating organisations overall** during the trial process

TRL distribution (what the trial actually reports)

For **age verification providers** (the most clearly reported group):

- **29 providers** assessed
- **21 providers at TRL 8–9 (high maturity, near deployment)**

Interpretation:

The AATT uses the standard **TRL 1–9 framework**:

TRL	Meaning
TRL 1–3	Early research / concept stage
TRL 4–5	Lab validation / prototype
TRL 6–7	Pilot / demonstration in relevant environment
TRL 8–9	Fully developed, tested, deployment-ready

The following providers were explicitly described as part of the **TRL 8–9 (top-tier) cohort**:

- VerifyMy
- AgeChecked
- IDVerse
- GBG
- iProov
- Yoti
- Persona
- Trust Stamp
- Luciditi
- Private ID
- ConnectID (Australian Payments Plus)biometricupdate

Specialist age assurance / identity providers

- Yoti
- Incode Technologies
- VerifyMy
- AgeChecked
- IDVerse
- Persona
- Trust Stamp
- Luciditi
- Private ID
- GBG

Biometrics / authentication / verification companies

- iProov

Digital identity and infrastructure providers

- Australian Payments Plus (**ConnectID**)
- Austroads (mobile driver's licence solutions)

Other notable participants and initiatives

- Civic
- Fujitsu
- VerifyMy
- euCONSENT (EU digital identity project)

Large platform / ecosystem participants

- Meta (including a joint involvement with Snap Inc.)
- Google (exploring wallet-based age credentials)
- Mastercard (referenced in trial participation discussions) [

Platforms restrict access to 4.7 million under-16 accounts across Australia

Share

16/1/26

Major social media companies removed access to about 4.7 million accounts identified as belonging to children under 16 in the first half of December to comply with Australia's social media minimum age, according to initial figures gathered by eSafety.

eSafety's focus since the minimum age obligation took effect on December 10 has shifted from preparation to monitoring and enforcement, concentrating on platforms assessed as age restricted and identified as having high under-16 usage in Australia.

The data released today is an early indication that major platforms are taking meaningful actions to prevent under-16s from holding accounts.

"I am very pleased with these preliminary results," eSafety Commissioner Julie Inman Grant said.

"It is clear that eSafety's regulatory guidance and engagement with platforms is already delivering significant outcomes."

While eSafety recognises the process of age assurance requires time to complete fairly and accurately, it has clearly articulated its expectations around continuous improvement of age assurance accuracy and efficacy from platforms. It is also the responsibility of industry to prevent circumvention, as outlined in eSafety's industry guidance.

eSafety Commissioner Julie Inman Grant acknowledged reports some under-16s accounts remain active and cautioned it was too early to determine whether progress so far constituted full compliance by platforms, however early signs were encouraging.

"While some kids may find creative ways to stay on social media, it's important to remember that just like other safety laws we have in society, success is measured by reduction in harm and in re-setting cultural norms," Ms Inman Grant said.

"Speed limits for instance are not a failure because some people speed. Most would agree that roads are safer because of them. Over time, compliance increases, norms settle, and the safety benefits grow."

"And while effective age assurance may take time to bed down, we've had incredibly positive initial feedback already from three of the largest age assurance providers who have told us that Australia's implementation of the social media minimum age has been relatively smooth and this was supported by proactive public education and communication about what to expect in the lead up to 10 December."

Ms Inman Grant said the true impact of the social media minimum age won't be measured in weeks or months but will likely be generational.

"We are still at the very beginning of this journey, and it is evident platforms are taking different approaches based on their individual circumstances, resulting in variations in the data and outcomes currently surfaced," Ms Inman Grant said.

"Of course, while some positive changes will be clearly evident today, some of longer-term normative changes and related positive impacts on Australian children and families may take years to fully manifest.

"This is precisely why eSafety is undertaking a longitudinal evaluation to measure these impacts over time. As previously announced, we will be measuring these impacts in collaboration with the independent Academic Advisory GroupExternal link," Ms Inman Grant said.

eSafety has been clear in its engagement and guidance to age-restricted social media platforms that services are required to self-assess in relation to whether they meet the legislative criteria, and to take reasonable steps to comply accordingly.

This messaging and engagement has resulted in services such as BlueSky and Lemon8 assessing themselves as meeting the criteria, and they are working cooperatively with eSafety.

“Given the vast number of online services and the fast-evolving nature of the tech industry, it’s impossible to list all of the services which meet the conditions and are obliged to comply with the social media minimum age obligation,” Ms Inman Grant said.

“As I have said for some time now, our compliance focus will remain on platforms with the highest number of Australian users.”

eSafety will continue gathering data, reports and information – including any indications of large-scale user migration to other platforms – to ensure compliance, safety and improve industry performance. So far, eSafety’s analysis has found that migration to other platforms has quickly spiked in terms of downloads but have not necessarily translated into commensurate usage.

eSafety will continue to build a more complete picture about platforms’ compliance with their legislative obligation to take reasonable steps ensuring under 16s do not have accounts on their platforms.

To maintain the integrity of its investigations, protect legal privilege and preserve the ability to take appropriate enforcement action where necessary, eSafety will not be publishing specific numbers or detailed information obtained using its information-gathering powers.

Information, resources and advice including eSafety’s regularly updated FAQs for families and young people are available on eSafety’s Social Media Minimum Age Hub.

For more information or to request an interview, please contact:

Phone: 0439 519 684 (virtual line – please do not send texts)
or media@esafety.gov.au

eSafety begins evaluation of Australia's world-first social media minimum age

Share

26/2/26

eSafety has commenced a comprehensive evaluation of Australia's world-first social media minimum age to understand how the new obligation on platforms is working in practice — and what impact it is having on children, young people and families.

This major study will assess how the minimum age is being implemented, examine both intended and unintended impacts, and deliver strong, evidence based insights to guide future decision making. It will also contribute valuable new knowledge to the global conversation about children and young people and social media and wellbeing.

The study will follow over 4000 children and families over more than two-years using a range of complementary research methods, including:

- surveys with children and young people aged 10–16 and their parents and caregivers interviews and group discussions exploring lived experiences
- opt-in, privacy protected smartphone use tracking, capturing high level information only (such as app use, time spent and time of day)
- linking of survey data to administrative datasets, including National Assessment Program – Literacy and Numeracy (NAPLAN), Medicare Benefits Scheme (MBS), and Pharmaceutical Benefits Scheme (PBS).

The study's design and evaluation instruments are available on the Open Science Framework (OSF)External link. These materials will be updated on an ongoing basis as the evaluation progresses to ensure full transparency.

The project is being led by eSafety's Research and Evaluation team in partnership with:

- Stanford University's Social Media Lab (lead academic partner)
- An Academic Advisory Group of 11 leading Australian and international experts in youth wellbeing, psychology, public health, education and technology

More detailed information about the evaluation has been added to eSafety's Social Media Minimum Age hub at eSafety.gov.au/SMARExternal link where regular updates will be provided. Updates are also available by subscribing to eSafety's research news External link
eSafety Commissioner Julie Inman Grant said the evaluation would include input from a diverse range of sources, including surveys of and discussions with young people themselves.

"We know young people are central to the evaluation that's why members of the eSafety Youth Council are helping shape the research and interpret emerging findings, ensuring young people's voices and experiences remain front and center," Ms Inman Grant said.

"This blended approach brings together academic expertise, youth insight and independent oversight to ensure the evaluation is rigorous, credible and grounded in real world experience."

The evaluation has received full ethics approval from the Australian Institute for Family Studies Human Research Ethics Committee and meets high standards of academic integrity, privacy and research conduct.

The study will explore a wide range of outcomes, including children's wellbeing and mental health, their exposure to online risks and harms, and their digital habits and social media patterns. It will also examine help seeking behaviour, family relationships and parenting experiences and, the early experiences and impacts on young people under 16.

Findings will be released progressively through public reports and peer reviewed publications starting later this year and across 2027 and 2028. Initial reports will focus on early experiences and impacts on young people under 16, with deeper and longer term analysis continuing over time.

A legislative review of the Social Media Minimum Age legislation will be conducted by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

eSafety expects evaluation outcomes will provide an evidence source alongside wider data, research and community input.

For more information or to request an interview, please contact:

Phone: 0439 519 684 (virtual line – please do not send texts)
or media@esafety.gov.au

Five social media platforms flagged for compliance issues

Share

31/3/26

eSafety has significant concerns about the compliance of Facebook, Instagram, Snapchat, TikTok and YouTube with Australia's Social Media Minimum Age (SMMA) obligation and is continuing to gather evidence necessary to inform potential enforcement action.

eSafety's first SMMA compliance report, published today, shows there has been some progress in the first 3 months, including large scale account removals and more visible underage reporting pathways.

However, insights from a range of sources including platforms' responses to legally enforceable information-gathering notices, public reporting and eSafety's pulse survey, show major gaps remain.

eSafety has observed a number of poor practices that give rise to compliance concerns outlined in today's report. These include:

- Prompting children to attempt age assurance even where their declared age prior to 10 December 2025 was under 16.
- Enabling children aged under 16 to repeatedly attempt the same age assurance method to ultimately obtain a 16+ outcome.
- Failing to provide accessible or effective pathways for reporting age-restricted accounts.
- Insufficient measures to prevent new under 16 accounts being created.

eSafety has notified the relevant age-restricted platforms about specific issues and expectations for improvement and warned it is currently investigating potential non-compliance.

"While social media platforms have taken some initial action, I am concerned through our compliance monitoring that some may not be doing enough to comply with Australian law," eSafety Commissioner Julie Inman Grant said.

"As a result, we are now moving into an enforcement stance. Any enforcement action requires sufficient evidence, which takes time to gather. The evidence must establish the platform has not taken reasonable steps to prevent children aged under 16 from having an account. That means more than simply demonstrating some children do still have accounts. Rather, the evidence must show the platform has not implemented appropriate systems and processes."

eSafety has a range of enforcement powers, including infringement notices, enforceable undertakings, public Platform Provider Notifications and civil penalties of up to $49.5 million.

While eSafety is releasing this update as part of our continued commitment to transparency, there will be some information we cannot share to maintain the integrity of our investigations and ensure any potential enforcement action is not compromised.

ENDS

Additional quotes attributable to Australia's eSafety Commissioner Julie Inman Grant:

"This reform is unwinding 20 years of entrenched social media practices.

"Durable, generational change takes time—but these platforms have the capability to comply today and we certainly expect companies operating in Australia to comply with our safety laws.

“They can choose to do so or face escalating consequences, including profound reputational erosion with governments and consumers globally.

“While the onus is on age-restricted platforms to take reasonable steps to keep children under 16 from having accounts, parents are proving pivotal partners in this cultural reset.

“We have heard from parents who have said the law is empowering them to say no to requests by their kids to have social media accounts.

“Any cultural change that pushes against the powerful interests and revenue potential of entrenched industry players - whether car manufacturers, Big Tobacco or Big Tech. Those players will push back but we continue to push ahead.

“We are committed to seeing further action taken by these social media giants, either through significant safety uplift in line with Australia’s laws, or in response to enforcement action.”

For more information or to request an interview, please contact:

Phone: 0439 519 684 (virtual line – please do not send texts)
or media@esafety.gov.au

FOLDER 2

GENERAL MANAGER - CORPORATE AND STRATEGY

Additional Estimates Information – May 2026

1	Key Issues briefs and key stats	1.1	Key Issues Briefs
		1.2	ACMA Key Issues – Budget
		1.3	Key Statistics
2	Additional items	2.1	Performance measures
		2.2	International Engagement
		2.3	eSafety's advice to MO on online hate
		2.4	eSafety's advice to MO on Roblox
		2.5	Proposed legislation about the Online Safety Act (note, not OSA review)
3	QoNs	3.1	eSafety QoNs
		3.2	ACMA/eSafety Coord QoNs (eSafety input)
4	Other [non indexed items]	4.1	Research List
		4.2	Extra Estimates
		4.3	2026 February Estimates

INSERT:

KEY ISSUES BRIEFS

ACMA KEY ISSUES BRIEF – Budget

KEY STATISTICS

2.1 Non-financial component – Performance Measures

Talking Points

- The 2024-25 eSafety Annual Report gives a clear picture of how we've performed this year – the progress we've made to protect Australians from online harm and create safer, more positive online spaces. It also meets our transparency obligations as a government agency.
- This year marked eSafety's tenth anniversary. In our tenth year, our purpose is stronger than ever, and so is our commitment to lead with care, determination, and impact.

How did eSafety perform against the targets set out in the 2024-25 Corporate Plan?

- In the 2024-25 Annual Performance Statement we reported against **16 performance measures** across **three key activity areas**.
  - Key activity 1: eSafety designs and delivers **educational materials** to prevent online harms, **working with key sectors and community members** to build user capability and resilience.
  - Key activity 2: eSafety **alleviates harms** through our **investigations and regulatory schemes**, in response to reported and identified harms.
  - Key activity 3: eSafety implements and enforces **industry regulatory measures** to drive proactive and systemic change in online safety.

- We **fully met 12** of our 16 performance measures, **partially met 2**, and **2 were not met.**

Changes in language in relation to Investigations Branch performance measures

- We have shifted away from references to **'informal request**s' and adopted the term '**voluntary request**' to clearly convey to industry that eSafety is asking them to **voluntarily review material** on their platform against their terms of service.
- **Service provider notifications** are statutory provisions to notify a platform of the existence of material on their service that meets a relevant threshold.
  - A SPN **does not require the platform to remove the material**, but gives them the opportunity to **proactively take action**.

Why was performance measure 2.1.1 (Successful action taken in at least 80% of cyber abuse complaints) only partially met?

- We fell just short of meeting our target for this performance measure, with **harmful content being removed** in response to **78% of complaint notifications.**
- **Complaint volumes** continue to increase.
  - More than 3,600 complaints assessed during the reporting period
  - Each complaint is reviewed by an investigator, including an assessment of the material, open-source research, and potential contact with platforms or other users.
- **Growing resistance** from some international platforms.
  - Shifting political conditions
  - Rolling back safety policies

- Our **expertise is growing** and we are exploring ways to provide public education that **reduces out of scope complaints**, allowing us to focus faster on the cases where we can act.

Why was performance measure 3.1.1 (All 8 industry sections have codes or standards registered for Phase 2 of the industry codes development) only partially met?

- Codes for all 8 industry sections were registered by **September 9 2025**.
- At the time of reporting the Commissioner had registered codes for **3 sectors**. Codes for the remaining 5 industry sectors were registered by the Commissioner on 9 September.
- This is a **co-regulatory scheme** and while we **maintain an active and collaborative role**, the responsibility for getting these codes right **rests with industry**.
- Code-making spans emerging technologies, complex platform behaviours and sensitive policy areas, such as child protection and illegal content.

Why was performance measure 3.2.1 (ten non-periodic reporting notices were issued) not met?

- In 2024-25 we used a **different mechanism** to **achieve the same outcome** more efficiently.
- We used **Information Requests under section 20 of the BOSE Determination** rather than non-periodic reporting notices.
    - These requests require **less lead time** than non-periodic notices which allowed us to analyse and publish findings in a shorter timeframe.
- This approach was enabled by the **May 2024 amendments to the BOSE Determination**.

Why was performance measure 3.2.2 (transparency summaries were published in relation to responses received to periodic notices) not met?

- Although not published by June 30, 2025, the transparency summary was **published in August** – a little more than one month after the official reporting window closed.
- The primary reason was a **delay in issuing the periodic notices** that the transparency summary is based on.
    - At the time the performance target was set, it was expected that these notices would be issued before the beginning of the reporting year. In fact, they were **not issued until July 2024**, with **responses not due until February 2025**.
    - The delay was the result of **pressures arising from ongoing enforcement action and legal challenges** relating to notices previously given. Also, the decision to prioritise notices on terrorism and violent extremism.

You report receiving 3,406 cyberbullying complaints but only contacted platforms in 848 cases. Why is this so low?

- This performance measure reflects cases where we were able to verify harmful content and intervene.
- While many complaints involve harmful content, some **do not meet the legal threshold** under the Online Safety Act.
- Other complaints involve content that has **already been taken down or expired**, such as on Snapchat or Instagram where material is designed to disappear

2.2 Intl' & advice to government (SER)

International Engagement

Global Online Safety Regulators Network (GOSRN)

- GOSRN brings together 31 organisations across 6 continents (9 regulators, 22 observers) to share information and insights and support coordinated approaches to online safety.
- In 2026, eSafety will chair a new 12-month GOSRN working group focussed on RegTech and regulatory innovation. The group is yet to meet and settle a terms of reference.
- In January 2026, GOSRN released a position statement on age assurance, which sets out fundamental principles countries' should consider when designing and deploying age assurance technologies.

Other International Engagement

- eSafety represents Australia on the Global Partnership for Action on Gender-Based Online Harassment and Abuse.
- eSafety also participates in and engages with other multilateral fora and bodies including WeProtect Global Alliance, OECD, INHOPE, UN bodies (UNICEF, UNFPA, UN Women, UNESCO), and the Asia-Pacific Economic Cooperation (including a self-funded project in 2025 on "Empowering Women and Businesses to have Safe Online Workspaces")
- Recent events include: US TrustCon2025, APEC SOM3 in Incheon South Korea, Pacific Cyber Week in Fiji, Standford Trust and Safety Research Conference, and ASEAN ICT Forum on Child Online Protection 2025.
- eSafety regularly meets with international partners to share its experience in online safety regulation, in particular noting the international focus on the social media minimum age obligation to share experiences.

2.3 eSafety's advice to MO on online hate

General talking points

- In response to the Bondi Beach Attack, the Government announced its intention to pursue a range of measures and initiatives to better address hate against groups. This included online hate, including online antisemitism.
- Upon request from the Minister, in February 2026, eSafety provided advice to the Minister on proposed measures to better address online hate under the Online Safety Act. eSafety's advice is with the Minister and Government for their consideration.
- eSafety also presented to the Standing Council of Attorneys General in February 2026 to share our regulatory insights and discuss ways to better address online hate through a nationally led approach.

Questions about the contents of eSafety's advice

- eSafety's advice is currently with the Minister and Government for their consideration. Accordingly, eSafety is not placed to speak to the details of the advice.
- However, we can note:
    - eSafety considers that an inclusive and holistic approach is best capable of promoting industry accountability, effective redress and social cohesion to address online hate, including antisemitism.
    - Addressing online hate, including antisemitism, should be bolstered by a regulatory response which places the onus on service providers to prevent such harm from occurring on their services and complemented by targeted education and training.
    - The Government has stated its intention that online hate will be addressed under the duty of care, which the Government has committed to as a top priority for introducing in the Online Safety Act. eSafety continues to work closely with the Government and Department in progressing this important reform.

s 47C

s 47C

2.4 eSafety's advice to the MO on Roblox

General talking points

- In February 2026, the Minister requested that eSafety provide advice on how to address harms to children on Roblox and similar gaming platforms. This followed concerns, including from the Government, about a range of serious and acute harms to children on Roblox, including child sexual exploitation and abuse, exposure to user-generated sexually explicit material, and exposure to suicidal material.
- In March 2026, eSafety provided advice to the Minister on a proposed approach to strengthening measures to address harms to children on Roblox and similar gaming platforms. eSafety's advice is with the Minister and Government for consideration.
    - Before the Minister's request, eSafety was already proactively monitoring and engaging with Roblox about their safety practices and compliance with their obligations under eSafety's regulatory schemes, including engaging with Roblox on its regulatory obligations prior to the commencement of the Relevant Electronic Services Standard in December 2024.
    - eSafety has continued to engage with Roblox and investigate their safety practices:
        - In February 2026, eSafety notified Roblox that in addition to our ongoing compliance monitoring, eSafety will be directly testing the implementation of Roblox's 9 commitments to support compliance under the Online Safety Act.
        - In April 2026, eSafety gave a transparency notice to Roblox and three other online game providers (Minecraft, Fortnite, and Steam) regarding how they are protecting children from exposure to a range of harms including child sexual exploitation and abuse, violence material and activity, cyberbullying, and online hate.
    - In its response to the OSA Review, the Government stated its intention to 'focus on protecting vulnerable Australians, including children, combating criminal activity and promoting public safety' under the duty of care. These harms would capture many of the harms occurring on Roblox and similar gaming platforms. eSafety continues to work closely with the Government and Department in progressing this important reform.

Questions about the contents of eSafety's advice

- eSafety's advice is currently with the Minister and Government for their consideration. Accordingly, eSafety is not placed to speak to the details of the advice.
- However, we can note there are a number of existing mechanisms under the Online Safety Act to address harms to children on Roblox and similar platforms. These include:
    - Unlawful material codes and standards – Relevant Electronic Services Standard
    - Age-restricted material codes – Relevant Electronic Services Online Safety Code
    - Basic Online Safety Expectations
    - Complaint schemes
- eSafety's advice builds on strengthening these mechanisms.
- eSafety's advice also aligns with the Government commitment to legislate a duty of care, by placing the onus on industry to keep their platforms safe for users. eSafety continues to work closely with the Government and Department in progressing this reform.

s 47C

[redacted]

s 47C

Further talking points on eSafety's investigation into Roblox is in Key Issues Brief – Codes and Standards. Further talking points on eSafety's non-periodic notice to gaming services is in Key Issues Brief – BOSE.

2.5 Proposed legislation about the Online Safety Act introduced in 2026

- As a regulator, eSafety's role is to enforce legislation as passed by Parliament. However, we monitor developments within Parliament as part of being an anticipatory and informed regulator.

Online Safety Amendment (Fix Our Feeds) Bill 2026 (introduced by Senator Hanson-Young)

- The Fix Our Feeds Bill seeks to require social media services to allow users to opt out of recommended content and for the Government to implement a duty of care. It draws upon the work of Teach us Consent.
- eSafety has highlighted the need for safer design of the whole platform, including recommender systems and algorithms.
- Updating a paper we first released in December 2022, this month we published an updated position statement on recommender systems and algorithms. It explores the current and emerging risks and harms, opportunities, regulatory challenges, and provides guidance on Safety by Design measures.
- The Government has committed to legislating a duty of care under the Online Safety Act. eSafety continues to work with the Department and Government to progress reform under the Online Safety Act review, including the development of the duty of care.

Further talking points regarding the duty of care are available under 'OSA Review'.

Online Safety Amendment (Broadening Adult Cyber Abuse Protections) Bill 2026 (introduced by Senator Payman)

- The Broadening Adult Cyber Abuse Protections Bill seeks to lower the threshold of the adult cyber abuse scheme.
- The Online Safety Act Review acknowledged the importance of our complaint schemes. We anticipate that our complaint schemes will continue to operate and complement the duty of care.

2.5 Questions on Notice

Print and insert the following

eSafety QoN Overview from February 2026.docx

and a copy of all the QoNs from this folder

a - QoNs from February Estimates

and this (which is 3.2 in the index)

eSafety Responses - Coord QoNs - February 2026 Additional Estimates (1).xlsx

4. Other

4	**Other** **[non indexed items]**	4.1	Research List [print this Research list.docx
		4.2	1. Extra Estimates [print this Extra Estimates .docx
		4.3	2. 2026 February Estimates [print this 2026 February Estimates.docx

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

GM BRIEF: KEY SAFETY IMPROVEMENTS and ONGOING INDUSTRY ENGAGEMENTS

Talking Points

- With thousands of online service providers in scope of the Online Safety Act, we established an industry supervision function to engage with industry on a 1:1 basis, and to build broader awareness of their regulatory obligations.
- Industry supervision is a form of proactive engagement with industry to achieve compliance with their regulatory obligations.
- This allows eSafety to move beyond ad hoc engagement and apply consistent oversight across a large number of services.
- Supervision is supported by data-led insights, tiered engagement and clear escalation pathways linking engagement to enforcement.
- Since 1 January 2026, we have held 57 meetings with online services and age assurance providers. Targeted engagement is delivering real safety uplift on services like Roblox, Discord and Snapchat.
- Despite some reporting indicating that children have moved to other online services as a result of the SMMA, eSafety has not observed any significant migration. We continue to keep a watching brief through market insights such as app download and site visit figures.

Key Issues

- eSafety's supervision function supports compliance and enforcement capability through proactive engagement to uplift compliance with the OSA. It contributes to a more coordinated industry engagement workplan, allowing enforcement teams to focus on enforcement activity.
- Engagement with services can be an on or off ramp to other enforcement options.
- Since 1 January to 30 April 2026, Safety has held 57 meetings with regulated entities, industry bodies and age assurance services on regulatory obligations.
- Engagement has focused on compliance with the Social Media Minimum Age obligation, Age Restricted Material Codes and Unlawful Material Codes and Standards.

1-Many supervision

- Since 1 January 2026, eSafety has hosted three industry webinars to raise awareness and understanding of obligations under the Online Safety Act. These webinars have targeted:
  - Services that allow pornography
  - AI chatbots to understand their obligations under the ARM Codes;
  - Tech Council of Australia members and partners
- eSafety has also delivered industry newsletters with updates across our regulatory schemes and a mass mailout reminder on 9 Mar that 6 of the ARM Codes are now in force.

Contact: s 22 Cleared: s 22 , Executive Manager

Phone: s 22 Date: 05/05/2026

1-1 supervision and supporting engagement

Service providers	Total branch meetings held with industry 1 Jan – 30 Apr 2026	Key issues discussed
Apple	3 March 1 April	• ARM Code compliance • CSEA reporting and detection gaps
Bytedance (TikTok, Lemon8 and CapCut)	21 Jan 19 Feb 10 March 23 April	• SMMA – TikTok and Lemon8 • ARM Code compliance – TikTok and CapCut • TVEC content on TikTok • Safety updates
Discord	30 Jan 25 March	• CSEA reporting and detection gaps • Product deep dive • Safety updates
Google	3 Feb 24 Feb 17 March 23 April	• SMMA (YouTube) • ARM Code compliance • CSEA reporting and detection gaps
Match Group	16 Jan 4 Feb	• Product deep dive
Meta	4 March 6 Feb 16 March 31 March 14 April 1 May	• ARM Code compliance • Nudify ads • SMMA • Reporting gaps
Microsoft	26 Feb	• ARM Code compliance • BOSE periodic notices • BOSE non-periodic notice (Minecraft)
Reddit	31 March	• SMMA
Roblox	26 Feb 4 March 24 March	• RES Standard compliance • Product updates • BOSE non-periodic notice
Snap	3 Feb 17 Feb 10 Feb	• SMMA • End to end encryption • CSEA detection gaps
Age assurance providers ConnectID k-ID Persona Privately Yoti Tremau	 17 Feb 8 Jan 28 April 14 Jan 22 April 3 Feb 14 Jan 17 March	• Product capabilities • Product interoperability • Usage insights • SMMA and ARM Code implementation insights

OpenAge	28 Jan	
Adult content platforms Aylo Faphouse Hammy Media Technius WGCZ	 5 Feb 3 March 3 March 5 March 25 Feb 4 March	• ARM Code compliance
AI Companions Chai Research Corp Character Technology Inc	 3 Feb 11 Feb	• BOSE non-periodic notice
Gaming Epic Games Valve	 19 Feb 24 Feb	• BOSE non-periodic notice
Industry bodies DIGI Tech Coalition Tech Council of Australia	 23 Jan 22 Jan 23 Jan	• CSEA tools • Awareness raising of regulatory obligations
Self-assessed age-restricted social media platforms Bigo Live Substack Yubo	 29 Jan 22 April 29 Jan	• SMMA
Other Spotify Coverstar Wikimedia	 14 Jan 5 Feb 9 Feb	• Codes and Standards compliance • SMMA
Webinars Adult content providers Generative AI providers Tech Council of Australia	 11 Feb 10 Feb 21 April	• ARM Code compliance • All regulatory schemes for TCA members

Key industry safety uplifts

Roblox (See Industry Codes and Standards brief for additional detail)

- In June 2025, following safety and compliance concerns raised by eSafety at a senior level, Roblox made nine commitments to support compliance with the codes and standards.
  - These commitments included introducing tools to prevent adult users from contacting under 16 users without parental consent, and more private default settings for accounts belonging to users under 16. Roblox chose to implement age-assurance measures to support its implementation of these commitments.
  - Roblox informed eSafety at the end of 2025 that it had delivered these commitments.
- eSafety has conducted testing to validate the implementation of Roblox's commitments and assess Roblox's compliance with its obligations more broadly.
- On 13 April 2026, Roblox introduced a default restricted model for users under 16. This is intended to limit under-16 users to age-appropriate experiences and content.

Discord

- Following information obtained through the BOSE periodic reporting process, eSafety has been engaging with Discord on gaps in its compliance with the BOSE, the ULM RES Standard and the ARM Codes (code service not yet confirmed). We are continuing this engagement but note some positive safety uplifts.

- Discord has recently implemented system level safety defaults for users, including:
  - Teen-appropriate default settings.
  - Age assurance for access to age-restricted spaces and content.
  - Message and friend request safety measures.
  - Sexually explicit and graphic content filters turned on by default.
- When applied effectively, system-level defaults can improve protection for younger users and reduce reliance on user-initiated safety settings.

ARSMPs (See SMMA brief for additional details)

- eSafety has engaged with a number of platforms about their implementation of the social media minimum age obligations, raising concerns about effectiveness as they became apparent through our information gathering notices and insights.
- Our engagements with platforms have led to some improvements being implemented.
- The age ratings of Snapchat, Facebook and Instagram have been updated from 13+ to 16+ on the Australian Apple App Store.
- Snap, Meta and TikTok have improved their underage user reporting pathways, including through increased discoverability and updates to language and Help pages.
- Based on our testing Google appears to have introduced age verification requirements when users aged 14–17 attempt to change their date of birth. Previously, age verification was only required for changes to 18+.

Migration and compliance monitoring

- eSafety uses available market intelligence on app downloads, site visits and search behaviour to understand the extent to which Australian users are engaging with particular online services and if users are migrating across services.
- This shows where services are growing, declining or experiencing short-term spikes.
- Tracking services over time allows eSafety to distinguish sustained risk from brief trends and to prioritise supervision, compliance and enforcement activity accordingly.
- This data-led approach helps eSafety focus effort where harm is most likely to emerge.
- eSafety continues to monitor and engage with services such as Pinterest to understand usage of their platform. Public information shows an upward trend of Australian's downloading Pinterest, however there is no indication this shift is from under 16 year olds.

SMMA

- eSafety observed short-lived spikes in app download figures for a small number of services, including Yubo, Yope and Bigo Live. These fluctuations appeared to reflect temporary shifts in user behaviour rather than sustained trends.
- In response to these observations, eSafety engaged with the relevant services to discuss their obligations under the Online Safety Act, including their responsibility to assess whether their service met the definition of an age-restricted social media platform.
- Each of these services self-assessed as being in scope and committed to taking reasonable steps to comply with their obligations.
- eSafety has continued to monitor app download and site visit data across a broader range of platforms to assess whether there is sustained migration of under-16 users.

- The available data indicates that increases in downloads on these services were brief and that overall download and usage levels remain low. There is no evidence at this time of sustained migration to any one alternative platform.

X Corp

- Media reporting from the Daily Telegraph raised concerns that Australian children under the age of 16 may be holding accounts on X, publicly identifying their age and location, and engaging with or being exposed to self-harm and disordered-eating content that may fall within the definition of class 2 material.
- eSafety wrote to X Corp to seek information on X Corp's compliance with the Social Media Minimum Age obligation.
- X Corp has responded and eSafety is considering next steps.

4Chan

- eSafety has not assessed whether 4chan meets the criteria of an ARSMP, including whether it has the sole, or a significant, purpose of enabling online social interaction between two or more end-users.
- The SMMA requires age-restricted social media platforms to take reasonable steps to prevent Australians under 16 from having accounts on their service. 4chan does not require accounts, and so access would not be affected by the SMMA obligation.
- As of 30 April 2026, 4Chan has received 25.3M site visits from Australian end-users over the last 12 months. In comparison, Facebook has received 2 billion and Reddit, 1.8 billion. 4Chan site visits are ~98% lower than Facebook and Reddit.

Substack

- eSafety has engaged with Substack to discuss its obligations under the OSA. This includes its obligations to comply with Online Safety Codes and Standards, and whether it considers the service needs to comply with the SMMa obligation.
- Substack has notified eSafety that it does not assess its service as meeting the conditions of an age-restricted social media platform under section 63C of the Act and therefore is not required to comply with the SMMA obligation.
- We are aware that Substack has introduced age assurance for Australian end-users. According to Substack, its terms of use have required users to be at least 16 years old for some time, and its use of age assurance is not due to the Social Media Minimum Age obligation. They are also not obligated to have age assurance under the Age-Restricted Material Codes, as they prohibit the posting of online pornography, self-harm and high-impact violence material.

SEMRush stats

Date	gab.com	4chan.org	watchpeopledie.tv	kiwifarms.st	reddit.com
Nov-25	17,629	1,630,953	71,356	175,019	143,564,609
Dec-25	35,058	1,511,048	142,308	145,352	146,832,425
Jan-26	30,600	1,545,546	247,575	135,067	153,006,340
Feb-26	30,832	1,350,135	317,197	136,295	122,441,091
Mar-26	30,037	2,302,495	414,258	215,312	165,156,095
Apr-26	39,191	1,508,658	95,904	175,484	135,689,806
Total	183,347	9,848,835	1,288,598	982,529	866,690,366

*Gab has previously been an app but not since 2021

These statistics were sourced from SEMRush and represent monthly Australian site visit data over the last 6 months (note that data is incomplete for May so was not included). These statistics represent total site visits (not unique user visits)

Gab's app download data was not included as it has not been available for download from the App or Play stores since 2021

Reddit stats have been included for comparison.

ARM Codes – safety uplifts in related to pornography service providers

- Prior to the introduction of the ARM Codes on 9 March 2026, eSafety began monitoring data on site visits for the most popular porn sites and AI chatbot apps and sites in Australia.
- We used this data to engage with services early, ensure awareness of their regulatory obligations and understand their plans to comply with the Codes.
- Industry Supervision use data led monitoring to prioritise the most visited sites and apply targeted engagement to secure compliance. We have identified the current top 30 sites for engagement and will continue this proactive approach as users move between sites.
- eSafety has directly engaged 26 pornography service providers who did not have age assurance in place, and continue to engage on uplifting compliance.
    - Approx 90% of the **most visited pornography sites by Australians in 2025** have introduced age assurance at the 18+ threshold. This reduces the risk of Australian children accessing pornographic material. Of the “top 5” pornography websites in Australia (Pornhub, xhamster, xvideos, xnxx and eporner) these sites have implemented age assurance differently:
        - Aylo has modified its free services in Australia, now providing free access only to a “safe for work” version of the site – paid access to online pornography on its services (i.e. age verified access) is still available.
        - The remainder of the top 5 (xVideos, xHamster, XNXX and ePorner) now require age assurance to access online pornography.

Most visited pornography sites in Australia (2025)

Platform name	Status
Pornhub; YouPorn; RedTube	Restricted access
Erome	AA in place
Faphouse	AA in place
xHamster; xHamster Live; xHamster44; xHamster Desi	AA in place
Spankbang	AA in place
Chaturbate	AA in place
Stripchat	AA in place
xVideos	AA in place
ePorner	AA in place

Background: Media articles – *If asked* responses

Commented [s 22]: This is really helpful - grateful if we could consider right up until the day if there are any further articles that we might need to address

Commented [s 22]:

Teen Aegis Posted on LinkedIn on 20 April, 2026 by Siobhan MacDermott, the founder and CEO of Teen Aegis – an 'intelligence' company for teen protection online.

Claim made in the post	eSafety response
70% of under-16s in Australia have social media accounts	• eSafety's research shows that 70% of under 16s who already had social media accounts before 10 December still have those accounts. It does not mean 70% of all under-16s currently use social media.
Under-16s migrated to Telegram (220,000 users cited)	• The 220,000 figure comes from South Korean data in 2024 about use of a specific deepfake channel. • The figure is unrelated to Australia and post-10 December behaviour. • There is no evidence of migration of Australian children to Telegram.
Under-16s migrated to anonymous video chat apps	• Short-term download spikes were observed around 10 December for apps such as Bigo Live and Yubo, but activity was not sustained. • eSafety engaged directly with both companies. Both self-assessed as ARSMPs and undertook compliance measures.
Under-16s migrated to Discord and it was excluded as an ARSMP by eSafety, by design	• Download and ranking data for Discord remained steady before and after 10 December. There is no evidence of a significant migration. • Discord was preliminarily assessed in November 2025 as not an ARSMP under the Rules made by the Minister.
Under-16s migrated to nudify apps	• No Australian download or usage data supports this claim. • Nudify apps are a strategic priority and eSafety is working with gatekeeper services to remove them. • There is no evidence of a link to the social media delay.
Instagram is not covered by the SMMA.	• Instagram is in eSafety's list of ARSMPs and is under investigation.

Children are moving to unregulated apps linked to fatalities (Character.AI, Telegram and Pinterest)	• Character.AI and Telegram have not been assessed under the criteria for ARSMPs. Pinterest was assessed in November 2025 as not meeting the conditions of an ARSMP. • All cited services remain subject to the Industry Codes and Standards, and have been engaged by eSafety.
eSafety does not track response times when families report harm	• The time it takes for services to respond to user reports of different types of harm has been collected and analysed through BOSE periodic and non-periodic reporting processes.
Platforms and eSafety acquired highly sensitive personal data for verification	• There are legislated controls on platforms' collection and use of data, supported by regulatory guidance issued by both the OAIC and eSafety. eSafety neither requires nor holds sensitive personal data for purposes of monitoring compliance with the SMMA obligation.

Cato Institute Posted on their site blog on 14 April, 2026. The Cato Institute are an independent public policy research organisation that promotes neo libertarian approaches for public policy.

Claim in the article	**eSafety response**
27% of parents reported their children moved to alternative or less regulated platforms	• The survey does not specify which platforms children moved to, what "moved" means, or what "less regulated" refers to. • The result reflects parent perception, not observed behaviour or usage data.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Codes and Standards

Talking Points

- eSafety established an Enforcement Taskforce in June 2025 to focus on investigating and enforcing non-compliance with the Online Safety Codes and Standards.
- Seventeen Codes and Standards are now in effect relating to unlawful material and age-restricted material.
- We have seen a number of positive outcomes from our Enforcement Taskforce including:
    - Roblox has put in place parental controls for users and default privacy settings for users who are under 16, supported by facial age estimation for all users. We are continuing to test and assess whether Roblox's safety measures are compliant with its obligations.
    - Chatroulette apps being removed from app stores
    - Improved terms of service for a model distribution service to minimise the risk of AI models producing child sexual exploitation material
- We have a number of other ongoing investigations concerning the availability of child sexual exploitation material including into allegations Grok may have been used to generate child sexual exploitation material.
- As a result of the Codes, age assurance measures have been adopted by the largest pornography providers in Australia.
- We are also engaging with the most used AI and companion services in Australia to seek their self-assessed risk profiles, the first stage of ensuring safety for children.

Key Issues

<u>Regulatory Priorities - Enforcement Taskforce</u>

- eSafety is prioritising four types of services for investigation and enforcement where required:
    1. Services with high risk and high prevalence of unlawful material and age-inappropriate material. This includes child sexual exploitation material and/or pro-terror content, or sites with the purpose of sharing online pornography.
    2. Services enabling adults access to children, resulting in self-generated imagery, grooming, sexual extortion and self-harm material.
    3. Generative AI models and services (in particular, 'nudify' services and AI Companion Chatbots) that can create child sexual exploitation material, online pornography, self-harm material and violence instruction material
    4. 'Gatekeeper' services, such as app stores and search engines, which enable access to a wide range of services/apps, including those that may be unresponsive to eSafety outreach.
- While these are eSafety's core priorities, eSafety will take broader action where the risk, evidence and need for deterrence supports it.

Contact: s 22
Phone:

Cleared by: s 22 ,
Head of Enforcement Taskforce
Date: 5 May 2026

Key Investigations

Grok and X

- In January 2026, eSafety commenced an investigation into **Grok, xAI's** generative AI service, after becoming aware of reports that it may have been used to create child sexual exploitation material, as well as image-based abuse of adults.
- eSafety is also investigating the **X** platform due to ongoing concerns about the prevalence of child sexual exploitation material and pro-terror material on the platform. Reports about Grok potentially generating child sexual exploitation material on X heightened these concerns.
- eSafety has sought information from both X Corp. and X.AI LLC as part of these investigations.
- Both services are required to have appropriate systems, processes and technologies in place to detect, remove, disrupt and deter their services from being used to disseminate child sexual exploitation material and pro-terror material, regardless of whether it is AI-generated.
- While eSafety can seek the removal of specific image-based abuse of adults using other regulatory powers under the Online Safety Act, the Unlawful Material codes and standards only cover generation and distribution of child sexual exploitation material, so cannot be used to address systemic issues related to image-based abuse involving adults. Further, Age-Restricted Material codes only prevent children's access to explicit adult images which may amount to image-based abuse, rather than the generation of such material.
- Beyond this, it is not appropriate to comment on an ongoing investigation.

Roblox

- eSafety has been engaging with Roblox on its regulatory obligations since prior to the commencement of the Relevant Electronic Services Standard in December 2024.
- As a result of this engagement, in June 2025, Roblox committed to implementing changes to better protect children in compliance with its mandatory requirements under the unlawful material codes and standards, following concerns raised by eSafety.
- These commitments included introducing tools to prevent adult users from contacting under 16 users without parental consent, and more private default settings for accounts belonging to users under 16. Roblox chose to implement age-assurance measures to support its implementation of these commitments.
- eSafety is concerned about ongoing reports of child sexual exploitation on Roblox, and has conducted testing to assess the implementation of Roblox's commitments and assess Roblox's compliance with its obligations more broadly.
- Beyond this, it is not appropriate to comment on the conduct of an ongoing investigation.

Joint Action – Nudify Services

- eSafety has identified several highly accessible services that openly market themselves as 'nudify' platforms. To avoid unintentionally alerting potential offenders, the names of the services and providers have been withheld.
- In April 2026, eSafety commenced investigations into several popular nudify services based on concerns that they had been used to generate child sexual exploitation material and online pornography, and that the services do not have appropriate age assurance.

- In May 2026, eSafety issued a formal Direction to Comply to one of the most popular 'nudify' services accessed in Australia, visited tens of thousands of times a month, giving the company 14 days to implement stronger age assurance protections to prevent children from accessing its service.
- Three of the most popular nudify services that withdrew access from Australia following our action last year have returned with a new owner, but have introduced age assurance. While we remain concerned about these services, and the Government has committed to ban them outright, we consider age-assurance does at least put in place some protections for children in the meantime as unfortunately, these services are often used by children against other children.
- eSafety is also considering the compliance of gatekeeper services, such as app stores and search engine services, with their obligations with respect to nudify apps and websites that their services make available.

Compliance and Enforcement Outcomes

- Through eSafety's compliance and enforcement activities to date, a number of services have made changes or committed to comply with the industry codes and standards.
- In relation to age-restricted material:
    - **Australia's largest pornography providers** have implemented measures to comply with the Age-Restricted Material Codes, approx. 90% of the most visited pornography websites in Australia introducing age assurance at the 18+ threshold, or other measures to comply:
        - Of the "top 5" pornography websites in Australia (Pornhub, xhamster, xvideos, xnxx and eporner) these sites have all implemented age assurance or other measures to comply:
            - Aylo has modified its free services in Australia, now providing free access only to a "safe for work" version of the site – paid access to online pornography on its services (i.e. age verified access) is still available.
            - The remainder of the top 5 (xVideos, xHamster, XNXX and ePorner) now require age assurance to access online pornography.
        - eSafety is live to the risk of migration and are monitoring this closely through our Industry Supervision function (see Industry Supervision brief) and engaging those services that are not yet in compliance.
        - However, based on data available to date, **there is no evidence of traffic consolidation or migration to a single service beyond the top five sites – they are still the biggest sources of online pornography in Australia**.
            - eSafety has also not observed peaks in VPN downloads that would solely account for the drop in user numbers across the top 5 services in particular.
        - eSafety has also engaged with high-risk services like Motherless, seeking urgent compliance information with both the Unlawful Material Codes and Standards and Age-Restricted Material Codes. Motherless has subsequently implemented age assurance for Australian end-users.
    - Gatekeeper services have begun implementing age assurance measures for Australians. E.g.:
        - **Google Search** has been implementing age assurance on Australians logged into an account since Q1. Accounts that are not age assured have filters for age-restricted material on by default.
        - The **Apple App Store** has been implementing age assurance since Q1 to block children in Australia from downloading apps rated 18+.

- In relation to unlawful material:
    - **Google Search** has implemented deterrent messaging, reporting and support information on Image Search, when users make search queries for terms with known associations to child sexual exploitation material.
    - A **random video chat service**, Thundr, that was the subject of multiple complaints to eSafety, has removed the ability for Australians to use the service in 'anonymous' mode, reducing the risk that it will be used to solicit child sexual exploitation material, following our engagement.
    - Another video-chat service **OmeTV app** has been removed by Apple and Google from their app stores. The provider of OmeTV has suspended all access, including to their website, from Australia.
    - Following our engagement, **Apple has removed or issued warnings to over 100** of these risky video chat apps and terminated the accounts of dozens of app developers.
    - **Hugging Face** has changed its terms of service so now all account holders are required to take appropriate steps to minimise the risks of models being used to generate child sexual exploitation or pro-terror material. Hugging Face is required to enforce these terms where there are breaches.

Age assurance under the ARM Codes

What constitutes appropriate age assurance?

- Under the Age-Restricted Material Codes, service providers are required to consider the technical accuracy, robustness, reliability and fairness of the solution/s they provide.
    - **Technical accuracy and reliability** – service providers should define acceptable error thresholds based on their risk, service type and user base, and be backed by accessible and timely appeal processes.
    - **Robustness** – the age assurance systems are secure and reasonably resistant to circumvention.
    - **Fairness** – the age assurance measures must be accessible and accurate for all end-users, factoring in bias, clear instructions and **provide multiple options** for age assurance methods.
- While the Codes do note that the use of photo identification or digital identity wallets to verify age is an example of appropriate age assurance, eSafety's regulatory guidance sets out its view that the use of government identification documents as the sole method to verify a user's age will not constitute appropriate age assurance as it will likely not satisfy the requirement of 'fairness' in the definition (acknowledging that some community members may not have access to identification).

How do the ARM codes safeguard user privacy?

- Any age assurance measures must comply with Australian Privacy Law, including the Privacy Act and the Australian Privacy Principles as regulated by the OAIC and ensure that impact on user privacy is proportional to the online safety objectives of the Codes. They must also minimise the collection of personal information.
- The Codes **do not** require services to implement systemic weaknesses into information security systems, verify the real identity of a user, disclose personal information of a user or take any other action prohibited under Australian law.
- eSafety and the Office of the Australian Information Commissioner have signed a Memorandum of Understanding which reflects on the imperative for coordinated regulatory responses for issues such as age assurance requirements under the Codes where privacy and online safety intersect.

Background

How many investigations do you have underway?

- As of 28 April 2026, we have 11 investigations under section 42 of the Act into industry codes and standards compliance. We also have a wider programme of compliance assessments and engagement are not formal investigations.
- It is not appropriate to comment on the detail of these investigations.

How do the codes and standards interact with the SMMA?

- The Codes and Standards apply to a large range of online services including social media services. Whether or not a social media service is an age-restricted social media platform, it will still be required to follow its obligations under the Codes and Standards.
- While the SMMA deals prevents children aged under 16 from having accounts online, the Codes and Standards apply a wider range of obligations to keep end-users safe – particularly child end-users - by requiring services to provide protections in relation to harmful material on their services.

Why have certain services (e.g., PornHub) chosen to withdraw from the Australian market?

- Aylo did not withdraw from the Australian market – they have limited their services to paid account holders only (who they can verify are adults) and still make available what is commonly referred to as "safe for work" material on their website, to lead to their paid content. This is a business decision they have made.
- Aylo, the provider of Pornhub and other pornography sites, was involved in the drafting process of the Codes and had ample opportunity to understand the requirements and implement age assurance for a broader customer base if it wished to.

Background on regulatory framework

- The Unlawful Material Codes and Standards seek to prevent and minimise harms from the worst material online. The requirements are limited to Class 1 material, which is defined in the Act as material that is, or is likely to be, classified as refused classification under the National Classification Scheme.
    - Class 1A material is defined in the industry codes and standards as the most harmful Class 1 material such as child sexual exploitation material, pro-terror material and 'extreme' crime and violence.
    - Class 1B material is defined as material that is still harmful, but less so than 1A, including crime and violence and drug-related material.
    - The industry codes came into effect between September 2023 and March 2024, and the industry standards came into effect in December 2024. An 'enforcement grace period' ended in June 2025.

- The Age-Restricted Material Codes seek to prevent children in Australia from accessing or being exposed to age-restricted material online, especially online pornography, self-harm material and high-impact violence material, and provide all users in Australia with tools to limit their exposure to this material.
    - The measures in the Age-Restricted Material Codes are risk proportionate, with the highest risk services often needing to implement appropriate age assurance measures before allowing access.
    - Many services are required to conduct risk assessments to assess the risk that children will use their service to access age-restricted material and follow obligations aligning with their risk profile.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Complaints Scheme

Talking Points
Bondi Beach Shooting

- eSafety's on-call capability was activated immediately following the Bondi Beach attack to monitor footage of the attack circulating online.
- eSafety also alerted platforms to ensure they were proactively responding to content on their platforms.
- Initial material depicting the shooting was classified as MA15+ by the Classification Board.
- Further material was subsequently classified as RC.
- **107 complaints** were received relating to footage of the Bondi Beach shooting.
- eSafety sought information from six providers (Meta, TikTok, Snap, YouTube, X Corp and Reddit) about their response to the attack and content that may be available on their services. All indicated they were removing content in accordance with their terms of service and had safety tools in place for under 18s for graphic content.

Royal Commission - Antisemitism

- **4 Adult Cyber Abuse complaints** tagged as antisemitism have been received this financial year.
- Material must target a specific Australian adult to be classified as adult cyber abuse. Many antisemitic complaints are directed at groups or communities rather than an individual and therefore fall outside this threshold.
- Some complaints also do not meet the threshold because the serious harm element cannot be established, where the material reflects strong disagreement or controversial views rather than a deliberate attempt to cause serious harm to an individual. The Act specifically states serious harm is more than mere ordinary emotional reactions such as those of only distress, grief, fear or anger.

Impact of the social media minimum age on Child Cyberbullying Complaints

- While less children are on social media, children are still online, including on messaging apps. The trend of increasing CB complaints continues, notwithstanding the social media minimum age.
- We have seen an increase in complaints about threats of violence, doxing and offensive/upsetting photos/videos but a decrease in complaints about nasty comments/name calling, unwanted contact, fake accounts/impersonation and meme pages
- Comparing complaint numbers received for the period 1 December 2024 - 22 January 2025 and 1 December 2025 - 22 January 2026 shows **a 15% increase**.
- Importantly the social media minimum age obligation does not appear to be deterring children from seeking help when they need it, even if the behaviour is occurring on an age-restricted social media platform.

Contact: s 22
Phone: s 22

Cleared by: s 22, Executive Manager
Date: 12/05/2026

Key Issues by Complaint Scheme

Image-Based Abuse

- eSafety received 6,664 image-based abuse reports during the reporting period 1 July 2025 to 31 March 2026, a 39% increase compared to the period 1 July 2024 to 31 March 2025.
- Sexual extortion was the highest category of harm, accounting for 49% of reports.
- eSafety received 100 reports involving digitally altered intimate images during the reporting period, a 186% increase compared to the same period in the last financial year (35). This type of content is commonly created with the use of nudifying apps, or more recently, AI tools.
- Identifying specific AI tool(s) used in the creation of intimate images is challenging. Images provided to or accessed by eSafety typically lack distinctive markers or traceable features that reliably indicate which particular tool or model was used in their generation. In some instances, there is sufficient information to indicate the tool used to create the image was also used to share it, but this is often not the case.
- 911 complaint notifications were given, 74% of which resulted in removal, and 23 service provider notifications (SPN) were given, 87% of which resulted in removal. *Note: there is no statutory requirement for content to be removed pursuant to complaint alerts or SPNs. Of the 911 complaint notifications, 428 related to URLs (79% full or partial removal), 472 relates to user accounts (69% removal) and 11 related to both URLs and user accounts (82% removal).*
- No removal notices have been issued under the scheme as content is often removed following a complaint notification or service provider notification. Additionally, 43% of reports involve threats to share intimate images, so there is no content to remove. Complaint notifications are an efficient and effective mechanism for facilitating rapid removal.
- Pornography sites, especially hack/leak/expose sites, account for most unsuccessful removal attempts. Many such sites often change Hosting Service Providers or use other intermediaries to hide their Hosting Service Providers. Automated scraping and bot-run sites also pose major challenges, often lacking human moderation. Other difficult platforms include uncooperative message boards, archive sites, file sharing services, and overseas-hosted services.

Illegal and Restricted Content

- Complaints to the Illegal and Restricted Content (IRC) team have an **increase of 48%** in URL's compared to the previous year.
    - eSafety has received a total of **14,222 complaints** for the current FY (Jul 2025 – Mar 2026) about material relating to CSAM. This is an **increase of 26%** compared to the same time previous FY.
    - eSafety has received a total of **1515 complaints** for the current FY (Jul 2025 – Mar 2026) about material related to TVEC. This is an **increase of 498%** compared to the previous FY. The increase can be attributed to reports of known material being re-posted such as footage of the Buffalo and Christchurch terrorist attacks as well as an increase in reports about material that relates to current world conflicts.
    - eSafety has received a total of **5,403 complaints** for the first half of the current FY (Jul 2025 – Mar 2026) about material relating to promotion, incitement or instruction in crime, violence, sexually explicit adult material, extreme or offensive content. This is an **increase of 97% compared** to the previous FY.
- Formal action by way of removal notices increased in the 2025-26 FY with **48 removal notices** issued - an **increase of 454%** compared to the previous FY.
    - 1 notice relating to CSAM material
    - 49 notices relating to TVEC and Crime and Violence

- 7 Revocation notices issued under section 113.

- The increase in removal notices is mainly due to those issued in response to the Bondi attack, other incidents of real-world violence and Operation Catalyst activities.

Bondi Beach Shooting

- Immediately following initial news reporting of the Bondi Beach shooting, eSafety proactively monitored for any footage of the attack circulating online to assess whether the content would meet the threshold for removal, which is Class 1 material or 'Refused Classification' as defined under the National Classification Scheme.
- A total of 107 complaints were received, mostly concerning uploaded bystander footage.
- Multiple videos of the attack and aftermath were quickly identified across platforms.
- eSafety also engaged with platforms to ensure they were being proactive in their own response to content on their platforms, including by removing violent content under their own terms of service and placing interstitials on gratuitous violence to prevent inadvertent or accidental viewing of the content.
- On 15 December, eSafety wrote to Meta, TikTok, Snap, YouTube, X Corp and Reddit requesting information on their response to the attack and content that may be available on their services. All providers responded to eSafety's information request and indicated they were removing content in accordance with their terms of service and had safety tools in place for under 18s for graphic content.
- Initial footage was assessed and referred to the Classification Board, which classified the material as MA15+.
- A later complaint containing new footage was classified by the Board as Refused Classification (RC).
- Investigations confirmed that the RC material had already been removed by Meta, so no removal notice was required.
- Additional materially similar RC content was identified on a fringe website and X; removal notices were issued. X geo-blocked the content however the content is still available on WPD. eSafety is considering what further action may be appropriate.
- X has lodged an application with the Classification Review Board to review the RC classification of the material subject to the removal notice. eSafety has made submissions to the Board in relation to the review. A decision is pending.
- eSafety has recently been alerted by an overseas regulator to 'gamified' versions of the incident circulating online overseas. The nature and origin of these is not clear and no content has been identified as available in Australia.
- eSafety is responding to a notice to produce documents and information to the Royal Commission into Antisemitism.

Adult Cyber Abuse

- eSafety received a total of 4239 Adult Cyber Abuse complaints (*3929 valid complaints*) during the reporting period, an increase of 66% compared to the same period in the last financial year. Only 2% of complaints are assessed as meeting the legislative threshold.
- Defamation accounted for 40% of all reports (valid and invalid), and 43% of valid complaints, making it the largest category. Defamation is not among the harms captured under the legislation.

- 7 Formal removal notices were issued during this period, resulting in 100% compliance in the removal of material
- 84 Service Provider Notifications were given, 80% of which resulted in content being removed.

Online Hate

- Hate speech was a recorded category in 49 complaints during the reporting period.
- Although online hate is not defined by the OSA through our complaint schemes, eSafety does receive complaints regarding online hate referring to content that attacks or discriminates against individuals or groups based on characteristics like race, religion, gender or disability.
- When receiving these types of complaints an assessment is made on whether the material meets the definition of 'serious harm', being serious physical harm or serious harm to a person's mental health, whether temporary or permanent but more than mere ordinary emotional reactions such as those of only distress, grief, fear or anger.
- For eSafety to act under the Adult Cyber Abuse or Child Cyberbullying schemes, the online hate complained of must target a specific Australian adult or child—not a group or organisation. However, if content promotes or depicts violence against a group, eSafety may act under the Online Content Scheme.
    - **4 Adult Cyber Abuse complaints** tagged as **antisemitic** received from July 2025 to present:
        - **Complaint** regarding numerous posts on X.com posted by an individual with a significant online footprint and a strong political position regarding the Israel/Gaza situation. This end-user targeted individuals with Jewish identities or those who publicly express pro-Israel views Assessment of the posts were that they would be regarded as offensive or malicious, however the serious harm element could not be established. Section 7 Definition not met.
        - **Complaint** where they were subjected to 'explicit antisemitic' abuse on social media. Material assessed as disagreeing views regarding Venezuela and the complainant was called a "zio-freak" however the serious harm element could not be established. Section 7 Definition not met.
        - **Complaint** where the complainant has been branded a liar and included screenshots of the complainants' comments which was posted to a pro-Palestinian Instagram account. The reported material is an Instagram 'Highlights' labelling certain accounts 'Zionists" No evidence of intention to cause serious harm. Section 7 Definition not met.
        - **Complaint** where the complainant was a teacher from a High School. A TikTok account had been created making fun of the teachers and senior executive at the school. The High School name was merged with Israel to create a new 'name' for the school. There was no evidence of intention to cause serious harm. Section 7 Definition not met.
- eSafety will be providing the Royal Commission on Antisemitism and Social Cohesion with a number of complaints about antisemitism in response to a notice to produce documents. These complaints were identified using wider search parameters aligned to the scope of the notice and are dated from 1 January 2022.

Children's Cyberbullying

- eSafety received a total of **2741** Children's Cyberbullying complaints *(2541 valid complaints)* during the reporting period, an **increase of 10%**.
- Nasty comments/serious name calling and offensive/upsetting pictures and/or videos remain the most prevalent categories of harm, accounting for 36% and 24% of complaints respectively.

- **248 Service Provider Notifications** were given, **96%** of which resulted in content being **removed**.
- A total of **3 removal notices** were issued - 1 removal notice was issued resulting in removal and 2 end-users removal notices were issued requiring end-users to refrain from posting further cyberbullying material. These matters were all successfully resolved.
- Few removal notices are issued under the scheme as content is frequently removed following a service provider notification with no further regulatory action required.

Complaints from Children under 16

- eSafety continues to receive complaints from children under 16 years of age
- Complaints typically decline over the December – January school holiday period, increasing in volume with the return to school
- Since implementation of the social media age restriction **10 December 2025 till 31 March 2026**, a total of **779** cyberbullying complaints relating to children under 16 were received, compared to **568** for the period of **10 December 2024 till 31 March 2025**. This is a marked increase of **37%** however, is maintaining the existing complaint volume trajectory over that period. This increase is mostly consistent with the overall complaint volume increase also occurring consistently with the other complaint schemes.

Other Issues

Reliance on the Classification Board to classify material

- **Q: How does eSafety determine whether material is class 1 under the Online Safety Act?**
  A: Class 1 material is material that has or is likely to be classified as Refused Classification under the National Classification Code. eSafety relies on the Classification Board to formally classify material as Refused Classification. eSafety can also determine that material is class 1 material on the basis that it is likely the Classification Board would classify it as such.
  Since X Corp's legal challenge during the Wakeley incident, eSafety has relied more on Classification Board decisions rather than making its own assessment that the material is likely to be classified as Refused Classification.
  More recently, X Corp challenged a Classification Board decision to classify footage of the Charlie Kirk assassination as Refused Classification.
- **Q: How long does the classification process take?**
  A: Applications are either standard, with up to a 20-business-day timeframe, or priority, with up to 5 business days, excluding weekends, public holidays and shutdown periods. There is no out-of-hours classification or advice mechanism.
- **Q: What impact do review decisions have on eSafety's enforcement powers?**
  A: Where the Classification Review Board changes a classification, eSafety may be required to change its regulatory response, including revoking any removal notices that were issued based on a previous classification.

Collective Shout

- In April 2025, the online advocacy group Collective Shout launched an open letter campaign demanding credit card companies and PayPal payments for games on Steam and itchi.io after identifying games they claimed had themes of rape, incest sexual violence and/or child abuse.

- eSafety received complaints relating to 7 members of Collective Shout where members reported themselves or other members being subject to online harm. Anonymous complaints were also received regarding harm directed at a Collective Shout member.
- Between 19 July 2025 and 24 February 2026, 54 complaints have been received for online harms directed at members of Collective Shout to eSafety's adult cyber abuse (ACA), image-based abuse (IBA), and online content scheme (OCS) teams.
- There have been 36 ACA complaints, of which only 9 met the threshold for adult cyber abuse. For 3 of these, material was no longer available online so there was no action for eSafety to take. For the remaining 6, section 93(1) service provider notifications were sent to platforms resulting in the removal of material by the platforms.
- There have been 14 IBA complaints received. 3 led to removal of intimate images that were posted online, 4 reported content, none of which met threshold of the IBA scheme, 6 related to content that was no longer accessible online, and 1 was a duplicate report. Some reported content was referred to the adult cyber abuse scheme and some reports related to multiple pieces of content, some of which did meet the threshold of the IBA scheme, and some of which did not.
- There have been 4 OCS complaints; one of these was an internal referral of an ACA complaint; this content was assessed as class 1 material with the content removed following ACA action; a second complaint resulted in 4 items of content assessed as class 1 material and removed from the service; content in a further complaint was assessed as not class 1 material, with one complaint for unwanted material received by a Collective Shout member – this material was assessed as not class 1 material, or class 2 material provided on a relevant service provided from Australia.
- Under the ACA and IBA schemes, where matters reported by members of Collective Shout to eSafety met the threshold of those schemes, information gathering notices were sent to the service platform requesting end user identity and contact information in relation to the account holders who posted the material. Where the information is provided by the service platform, this information can be disclosed to relevant law enforcement under the Act.
- eSafety has disclosed (with consent) information to Australian Federal Police – Joint Policing Cybercrime Coordination Centre of these complaints along with additional information that was obtained by eSafety exercising a power under the OSA for these matters.
- One complaint identified conduct suspected to be criminal in nature, which has been referred to Victoria Police, who have state-based jurisdiction.
- eSafety also encouraged Collective Shout to report to law enforcement.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Corporate Matters

Talking Points

- The **2026-27 Budget** contained the following eSafety impacts:
  - One year continued funding of the Technology-Facilitated Abuse Support Service.
  - One year continued funding of the National Strategy to Prevent and Respond to Child Sexual Abuse Program.
  - Further reductions in spending on Consultants, Contractors and Labour Hire, and Non-wage Expenses.
  - Funding from existing eSafety resources prioritised to strengthen engagement with the Government, the Department and the Special Envoy to Combat Antisemitism

- eSafety has a **departmental** appropriation budget of **$66.5m** for the **2026-27** financial year

  (this includes departmental funding, ACMA direct appropriation, other revenue and depreciation expenditure)

- eSafety has an **administered** budget of **$3.5m** for the **2026-27** financial year

- eSafety has **236 full time equivalent** APS staff as at 30 April 2026

Key Issues

The **2026-27 Budget** includes the following impacts:

1. **Technology Facilitated Abuse Support Service**
   Funding of **$5.434m** for 2026-27.
   One year extension of the Technology-Facilitated Abuse Support Service to assist frontline workers and victim-survivors to navigate and respond to tech-facilitated abuse

2. **National Strategy to Prevent and Respond to Child Sexual Abuse**
   Funding of **$0.656m** for 2026-27.
   One year extension of the program that focuses on safeguarding children and young people from online harm, including sexual abuse and exploitation through resources, guidance and training.

3. **Government Response to the Antisemitic Bondi Attack**
   Part of a broader package "Government Response to the Antisemitic Bondi Terrorist Attack" [$207.4 million over five years from 2025-26 (and $8.1 million ongoing) to combat

---

Contact s 22
Phone:

Cleared by: s 22, General Manager
Date: 19/05/2026

the influences of antisemitism, violent extremism and hate in Australian communities, and respond to the recommendations of the Special Envoy's Plan to Combat Antisemitism.

The Government committed to support eSafety in providing online safety advice to address antisemitism following the Bondi terrorist attack.

$1.0 million in 2025–26 was prioritised from eSafety's existing resources to strengthen engagement and provide advice and support to the Government, the Department and the Special Envoy to Combat Antisemitism to enhance regulatory responses to online hate and progress duty of care reforms under the Online Safety Act.

Resource efforts have also focussed on:

- analysis and responding to online hate complaints,
- strengthening partnerships and sharing intelligence with federal, state and territory law enforcement agencies facilitating the rapid referral of harmful material,
- ongoing review of online abuse support materials,
- sharing regulatory insights and advice to better address online hate (eg work with Standing Council of Attorneys General), and
- responding to requests from the Royal Commission on Antisemitism and Social Cohesion.

4. **Further Reducing Spending on Consultants, Contractors and Labour Hire, and Non-wage Expenses - one year extension**
   Funding reduction of $1.871m
   One year extension, in 2029-30 financial year, of the 2025-26 Budget measure *'Savings from External Labour – extension'*.

Portfolio Budget Statements 2026-27

Table 1.2: Entity 2026-27 Budget measures

Part 1: Measures announced since the 2025-26 Mid-Year Economic and Fiscal Outlook (MYEFO)

	Program	2025-26 $'000	2026-27 $'000	2027-28 $'000	2028-29 $'000	2029-30 $'000
Payment measures						
Government Response to the Antisemitic Bondi Attack	1.3					
Departmental payment		nfp	nfp	nfp	nfp	nfp
Women's Safety-Ending Gender - Based Violence	1.3					
Departmental payment		-	5,434	-	-	-
National Strategy to Prevent and Respond to Child Sexual Abuse	1.3					
Departmental payment		-	656	-	-	-
Further Reducing Spending on Consultants, Contractors and Labour Hire, and Non-wage Expenses – One year extension [(b)]	1.1,1.2,1.3					
Departmental payment		-	-	-	-	*(6,800)

*Note: eSafety's component of the $6.800m reduction is **$1.871m**.

	2025-26 Estimated actual $'000	2026-27 Budget $'000	2027-28 Forward estimate $'000	2028-29 Forward estimate $'000	2029-30 Forward estimate $'000
Program 1.3: Office of the eSafety Commissioner					
Administered expenses Ordinary annual services					
Appropriation Bill (No. 1)	1,750	3,500	-	-	-
Administered total	**1,750**	**3,500**	**-**	**-**	**-**
Departmental expenses Departmental appropriation s74 External Revenue[a]	66,474	65,653	57,708	54,467	55,368
Special Account	390	300	-	-	-
Appropriation receipts[d]					
less expenses made from appropriations credited to special accounts[e]	59,386	58,580	50,636	47,395	48,296
Expenses not requiring appropriation in the Budget year[b]	(59,386)	(58,580)	(50,636)	(47,395)	(48,296)
Departmental total	1,687	514	373	12	-
Total expenses for Program 1.3	**68,551**	**66,467**	**58,081**	**54,479**	**55,368**
	70,301	**69,967**	**58,081**	**54,479**	**55,368**

Table 2.1.1: Budgeted expenses for Outcome 1

Table 2.1.1 breakdown

2026-27 PBS	2025-26 Estimated actual $m	2026-27 Budget $m	2027-28 Budget $m	2028-29 Budget $m	2029-30 Budget $m
Grants	1.750	3.500	0.000	0.000	0.000
Administered Total	**1.750**	**3.500**	**0.000**	**0.000**	**0.000**
Base funding (inclusive of savings measures)	46.593	46.655	46.502	47.395	48.296
NPP eSafety General awareness Initiative	0.100	0.100			
NPP Be Connected	4.034	4.082	4.134		
NPP National Strategy to Prevent Child Sexual Abuse	0.644	0.656			
NPP TFA Technical Support	5.600	5.434			
NPP Protecting Australians Online	1.633	1.653			
NPP Internal Legal and Compliance	0.782				
Total Departmental Appropriation receipts	**59.386**	**58.580**	**50.636**	**47.395**	**48.296**
External revenue	0.390	0.300			
ACMA net appropriation	7.088	7.072	7.072	7.072	7.072
Expenses not requiring appropriation (depreciation)	1.687	0.514	0.373	0.012	
Departmental Total	**68.551**	**66.467**	**58.081**	**54.479**	**55.368**
Total expenses for Program 1.3	**70.301**	**69.967**	**58.081**	**54.479**	**55.368**

Staffing

Employment type	As at 30 April 2026	As at 30 April 2025	Variance	Percentage change
APS (FTE)	236	194	42	22% increase
Contractors (FTE)	20	44	-24	55% decrease
Total	**256**	**238**	**18**	**8% increase**

- The growth in APS staffing numbers represents an increase in staff associated with new programs, primarily the SMMA NPP.
- The reduction in contractors represents the conversion of contractor roles to APS roles as per the Government's Strategic Commissioning Framework, and the conclusion of some contracts.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Online Hate including antisemitism

Talking Points

- Online hate, including antisemitism, is not explicitly covered in the Online Safety Act, but eSafety can act when content meets thresholds within other schemes (e.g. cyber abuse, industry codes, Basic Online Safety Expectations).
- Following the Bondi Beach attack, eSafety has strengthened engagement with Government, the Department, and the Special Envoy to Combat Antisemitism to enhance regulatory responses to online hate and progress duty of care reforms under the Online Safety Act.
- **107 complaints** were received relating to footage of the Bondi Beach shooting.
- Upon request from the Minister, eSafety provided advice to the Minister on proposed measures to better address online hate under the Online Safety Act. This is with the Minister and Government for their consideration.
- During the reporting period 1 July 2025 to 31 March 2026, eSafety received 49 Adult Cyber Abuse complaints categorised as hate speech and 4 complaints tagged as antisemitism—none of which met the Adult Cyber Abuse threshold.
- eSafety considers that an inclusive and holistic approach that addresses all forms of online hate and that promotes and requires systemic industry accountability is best capable of effectively and meaningfully addressing online hate in all forms.

Key Issues

eSafety's current approach and regulatory measures to address online hate, including antisemitism

- Since the Bondi Beach attack, eSafety has worked with Government, the Department, and other stakeholders, including the Special Envoy to Combat Antisemitism, to strengthen measures addressing online hate.
- Guidance on online abuse is available on eSafety's website and can support people experiencing online hate.
- eSafety has strong referral arrangements with law enforcement, including a joint initiative focused on online threats and extremism, such as antisemitic content.

Possible reform to address online hate, including antisemitism

- In response to the Bondi Beach Attack, the Government announced its intention to pursue a range of measures and initiatives to better address hate against groups. This included online hate, including online antisemitism.
- Upon request from the Minister, in February 2026, eSafety provided advice to the Minister on proposed measures to better address online hate under the Online Safety Act. eSafety's advice is with the Minister and Government for their consideration.

Contact: s 22
Phone: s 22

Cleared by: s 22, General Manager
Date: 19/5/2026

- eSafety also presented to the Standing Council of Attorneys General in February 2026 to share our regulatory insights and discuss ways to better address online hate through a nationally led approach.

- The Government has stated its intention that online hate will be addressed under the duty of care, which the Government has committed to as a top priority for introducing in the Online Safety Act. eSafety continues to work closely with the Government and Department in progressing this important reform.

Royal Commission into Social Cohesion and Antisemitism

- eSafety is in the process of complying with a Notice to Produce and Notice to Give a Statement in Writing from the Royal Commission into Antisemitism and Social Cohesion.
- eSafety was not mentioned in the Royal Commission's interim report and nor was online safety a strong focus. The report discussed **online extremism and radicalisation** at a high level, with mention of **AI, social media, online gaming** and **encrypted messaging**. The report also flagged online safety will be **a subject of consideration at the Commission's future hearings**.
- eSafety will continue to support the Royal Commission as required.
- If pressed:
    - It remains open to the Royal Commission to issue further notices, either for production of documents or for a statement. All parties would need to respond independently.
    - eSafety can't comment further. This is to ensure responses to current and future notices are prepared independently and not informed or influenced by comments made by other entities. Further, we want to avoid any adverse impression or perception about the independence or integrity of evidence provided by various parties, including different parts of the Commonwealth.

Overview of complaints related to antisemitism/online hate

- Hate speech was a recorded category in **49 ACA complaints** during the reporting period.
- Although online hate is not defined by the OSA through our complaint schemes, eSafety receives complaints regarding online hate referring to content that attacks or discriminates against individuals or groups based on characteristics like race, religion, gender or disability.
- When receiving these types of complaints an assessment is made on whether the material meets the definition of 'serious harm', being serious physical harm or serious harm to a person's mental health, whether temporary or permanent but more than mere ordinary emotional reactions such as those of only distress, grief, fear or anger.
- For eSafety to act under the Adult Cyber Abuse or Child Cyberbullying schemes, the online hate complained of must target a specific Australian adult or child—not a group or organisation.
- For content promoting or depicting violence against a group, eSafety may act under the Online Content Scheme.

ACA complaints tagged as antisemitic (July 2025–present):

- **Complaint** regarding numerous posts on X.com posted by an individual with a significant online footprint and a strong political position regarding the Israel/Gaza situation. This end-user targeted individuals with Jewish identities or those who publicly express pro-Israel views. Assessment of the posts were that they would be regarded as offensive or malicious, however the serious harm element could not be established. Section 7 Definition not met.

- **Complaint** where they were subjected to ‘explicit antisemitic’ abuse on social media. Material assessed as disagreeing views regarding Venezuela and the complainant was called a “zio-freak” however the serious harm element could not be established. Section 7 Definition not met.
- **Complaint** where the complainant has been branded a liar and included screenshots of the complainants’ comments which was posted to a pro-Palestinian Instagram account. The reported material is an Instagram 'Highlights' labelling certain accounts ‘Zionists’ No evidence of intention to cause serious harm. Section 7 Definition not met.
- **Complaint** where the complainant was a teacher from a High School. A TikTok account had been created making fun of the teachers and senior executive at the school. The High School name was merged with Israel to create a new ‘name’ for the school. There was no evidence of intention to cause serious harm. Section 7 Definition not met.

Background/Difficult questions

Questions about how eSafety’s regulatory measures address online hate, including antisemitism

- eSafety can issue removal notices where content meets legislative thresholds for cyber abuse or cyberbullying—targeting must be toward a specific Australian individual.
- Material showing or encouraging terrorist acts/extreme violence can be actioned under the Illegal and Restricted Content scheme. For example, eSafety has the power to assess complaints, or investigate certain matters on our own initiative, and decide what action we can take.
- eSafety enforces industry codes and standards across eight sectors to reduce systemic availability of harmful material.
- Transparency powers allow eSafety to request information.
    - eSafety published a report in 2024 about online hate on X and a report in 2025 about terrorist and extremist material.
    - On 1 April 2026, eSafety gave 4 non-periodic notices to the providers of online gaming services (Roblox, Fortnite, Minecraft and Steam) under the Basic Online Safety Expectations.
        - The notices require these online gaming providers to explain how they’re identifying, preventing and responding to matters including violent extremism.
        - The notices were given following public reporting to eSafety and media reports of terrorist and violent extremist-themed gameplay, and recreations of mass shootings on Roblox and far-right groups recreating fascist imagery in Minecraft.

Questions about eSafety’s view on online safety reform to address online hate

- eSafety supports industry-wide uplift in responding to all forms of online harm, including online hate.
- The Government has committed to a duty of care under the Online Safety Act, which the Minister has stated will address online hate.
- eSafety continues to work with the Department and Government on Online Safety Act reforms, including the duty of care.

Questions about eSafety's engagement with law enforcement

- eSafety has established partnerships with federal, state, and territory law enforcement agencies facilitating the rapid referral of harmful material. This includes complaint referrals to the AFP's Special Operation Avalite.
- Ongoing shared intelligence informs regulatory actions on terror/extreme violent content.
- eSafety refers matters to law enforcement where criminal investigation is appropriate.

Questions about eSafety's response to the Bondi Beach terror attack

- eSafety monitored for attack footage, assessed complaints, and engaged with platforms to remove violent material that met the threshold for removal (Class 1 material or 'Refused Classification' as defined under the National Classification Scheme.)
- **107 complaints** were received relating to footage of the Bondi Beach shooting.
- On 15 December, eSafety wrote to six platforms requesting information on their response to the attack and content that may be available on their services. These platforms included Meta, TikTok, Snap, YouTube, X Corp and Reddit.
- All platforms responded to eSafety's information request and indicated they were removing content in accordance with their terms of service and had safety tools in place for under 18s for graphic content.
- Refused Classification content was identified on a fringe website, which we won't name to avoid giving it any traffic or notoriety, and X; removal notices were issued. X geo-blocked the content however the content is still available on the fringe site.

Questions about the Special Envoy to Combat Islamophobia's report (National Response to Islamophobia)

- Implementation decisions are matters for Government.
- The report also calls for strengthened responses to online hate.
- Policy and legislative matters sit with the Department.

Questions about eSafety's contribution to the Royal Commission on Antisemitism and Social Cohesion

- eSafety is complying with a Notice to Produce and Notice to Give a Statement in Writing from the Royal Commission into Antisemitism and Social Cohesion.
- eSafety will continue to support the Royal Commission as required.

Questions about eSafety's contribution to the Commonwealth Inquiry into racism, hate and violence directed at Aboriginal and Torres Strait Islander people

- eSafety made a submission to this inquiry.
- eSafety research from a nationally representative survey conducted in November 2022 found that First Nations adults were significantly more likely to have been targeted with online hate.
    - Over 1 in 3 First Nations adults (34%) had personally experienced online hate in the 12 months prior to November 2022, compared with 17% of non-Indigenous adults.
    - 57% of First Nations adults had seen online hate in the previous 12 months, compared with 33% of non-Indigenous adults.
- eSafety supports industry-wide uplift in responding to online hate and continues to work closely with the Government to implement systemic uplift and reforms.

Antisemitic complaints and suggested response:

Why do some antisemitic complaints not meet the cyber abuse threshold?

- The OSA requires that material targets a *specific* Australian adult (s36). Many complaints relate to groups, not individuals.
- Some do not meet the "serious harm" requirement (s7), particularly where content reflects strong disagreement or political argument rather than intent to cause serious harm. To note:
  - The definition of serious harm is a legislative definition that was set with a high threshold when passed by Parliament.
  - Serious harm means serious physical harm or serious harm to a person's mental health, whether temporary or permanent.
  - Serious harm to a person's mental health includes:
    - serious psychological harm; and
    - serious distress

    It does not include mere ordinary emotional reactions such as those of only distress, grief, fear or anger.

2026-27 Budget Papers

$1.0 million in 2025-26 to the Australian Communications and Media Authority for the eSafety Commissioner to provide online safety advice to address antisemitism

- Part of a broader package "Government Response to the Antisemitic Bondi Terrorist Attack" [$207.4 million over five years from 2025-26 (and $8.1 million ongoing) to combat the influences of antisemitism, violent extremism and hate in Australian communities, and respond to the recommendations of the Special Envoy's Plan to Combat Antisemitism.

- The Government committed to support eSafety in providing online safety advice to address antisemitism following the Bondi terrorist attack.

- $1.0 million in 2025–26 was prioritised from eSafety's existing resources to strengthen engagement and provide advice and support to the Government, the Department and the Special Envoy to Combat Antisemitism to enhance regulatory responses to online hate and progress duty of care reforms under the Online Safety Act.

- Resource efforts have also focussed on:
  - analysis and responding to online hate complaints,
  - strengthening partnerships and sharing intelligence with federal, state and territory law enforcement agencies facilitating the rapid referral of harmful material,
  - ongoing review of online abuse support materials,
  - sharing regulatory insights and advice to better address online hate (eg work with Standing Council of Attorneys General), and
  - responding to requests from the Royal Commission on Antisemitism and Social Cohesion.

Australian Government | eSafetyCommissioner

2025 – 2026 Budget Estimates – May 2026

Environment and Communications

KEY ISSUES BRIEF: Social Media Minimum Age - Evaluation

Talking points

- The evaluation is designed to provide **robust evidence on both the intended and unintended impacts** of the legislation with **independent scientific oversight** from Stanford University's Social Media Lab and an Academic Advisory Group.
- The study follows **4,121** children and families.
- It examines **knowledge** and **attitudes** towards the SMMA, **adherence** behaviours, **digital use**, exposure to **risks**, child and family **wellbeing**, and **norms** around social media use.
- Baseline and second wave survey data have been collected and are being prepared for analysis. The **first public report will be released in Quarter 3 2026** and will present descriptive findings focusing on **baseline conditions** and **short-term behavioural indicators**.
- **Transparency is built in** through publication of research materials on the Open Science Framework, publication of Academic Advisory Group minutes, and progressive release of findings through public reports and peer-reviewed academic publications.
- **Strong ethical and data safeguards underpin the evaluation**, including ethics approval and informed consent from parents and children.

Key issues

Timing and communication of evaluation findings

- The SMMA evaluation is designed as a longitudinal study, with results released progressively between 2026 and 2028. As a result, definitive conclusions will not be available in the short term, particularly for complex outcomes such as wellbeing, family functioning and social norms
- Early findings will be descriptive, focusing on baseline conditions, implementation context and short-term behavioural indicators, rather than drawing conclusions about longer-term impacts.
- The current status is that baseline data and the second survey wave have been collected and are now being cleaned and prepared for analysis.
- The first public report is expected in Quarter 3, 2026, and will focus on methodology and early insights rather than definitive outcome measures.

Contact: s 22
Phone:

Cleared by: s 22, General Manager
Date: 19/5/2026

Independence, transparency and credibility

- The core purpose of the evaluation is to provide objective, robust evidence on both the intended and unintended impacts of the Social Media Minimum Age legislation.

- eSafety is leading the evaluation with independent oversight provided by the lead academic partner (Social Media Lab, Stanford University) and the Academic Advisory Group (AAG). Together they provide methodological and scientific oversight and lead the scientific reporting stream. Neither the Lead Academic Partner nor AAG members are remunerated.

- Transparency is a central design feature:
  - Study protocols, instruments and analysis plans are published on the Open Science Framework
  - AAG Terms of Reference and meeting minutes are publicly available on our website
  - Findings will be released progressively through two complementary streams
    - public reports led by eSafety
    - peer-reviewed academic publications led by Stanford and the AAG.

- Strong ethical safeguards underpin the evaluation:
  - Approval by an Australian Institute of Family Studies Human Research Ethics Committee
  - Informed consent from both parents/carers and children
  - Strictly opt-in participation for sensitive components of the study
  - Robust data governance arrangements supported by AIFS, an Australian Government-approved Integrating Authority and Accredited Data Service Provider.

Background

Purpose and scope

- The evaluation is designed to provide a robust assessment of the implementation and outcomes of the Social Media Minimum Age (SMMA). Its primary objectives are:
  - assess both the intended and unintended impacts of the legislation on children and their caregivers
  - provide objective, robust evidence to inform the independent review of the legislation
  - contribute to the global evidence base on social media age restrictions
  - advance knowledge in Australia on the relationship between social media use and youth wellbeing.

- The evaluation will measure change across a number of domains, including:
  - Knowledge about and attitudes towards the SMMA
  - Adherence and circumvention behaviours
  - Digital engagement, literacy, and habits
  - Exposure to online risks and harms
  - Child wellbeing and functioning
  - Family functioning, digital parenting and conflict
  - Norms around social media use in childhood and adolescence

Evaluation design

- The study follows more than 4,100 children and families. It will be conducted over an initial period of two years, with potential to extend for an additional three years. It uses a mixed-methods longitudinal design, comprising:
  - Multi-wave online survey

    - Qualitative research, including focus groups and interviews
    - Objective data collection, including passive tracking of smartphone usage (with informed consent)
    - Data linkage with administrative datasets (NAPLAN, PBS, MBS), where consent is provided.

- Data was collected at baseline, with follow-ups at ~3, 6, 12 and 24 months post-implementation.

Ethics and safeguards

- Strong ethical and participant safeguards are integral to the evaluation:
    - all methods involving sensitive data are voluntary and subject to strict ethical and consent requirements
    - the study has approval from an Australian Institute of Family Studies (AIFS) Human Research Ethics Committee
    - informed consent is required from both parents/carers and participating children
    - passive tracking and data linkage are strictly opt-in and require separate consent
    - declining passive tracking or data linkage does not affect participation in other components of the study
    - strong data governance arrangements are in place, supported by AIFS, one of the Australian Government's four approved Integrating Authorities and Accredited Data Service Providers (ADSPs)
    - help-seeking and support information is provided to participating parents and children.

Governance and transparency

- The evaluation operates under a hybrid governance model:
    - eSafety is responsible for overall leadership and delivery of the evaluation
    - Stanford University's Social Media Lab has been appointed as Lead Academic Partner
    - an Independent Academic Advisory Group (AAG), comprising national and international experts, provides methodological and scientific oversight.

- Neither the Lead Academic Partner nor AAG members are remunerated for their roles.

- Transparency measures include:
    - publication of the AAG Terms of Reference and meeting minutes on the eSafety website
    - publication of the study protocol, survey instruments and analysis plans on the Open Science Framework (with analysis plans pre-registered)
    - progressive release of public-facing methodology, cohort and findings reports, reviewed by the AAG
    - publication of peer-reviewed academic papers.

Reporting

- Indicative timing of public reports is as follows:
    - Quarter 3 2026 – Baseline and Wave 2
    - Quarter 4 2026 – Wave 3

- Quarter 2 2027 – Wave 4
- Quarter 2 2028 – Wave 5

Cost

The expected cost of the longitudinal survey is $1,460,839.00 (GST inclusive.)

Academic Advisory Group

Members of the Lead Academic Partner

- Professor Jeff Hancock, Stanford University Social Media Lab
- Dr Sunny Xun Liu, Stanford University Social Media Lab
- Dr Anja Stevic, Stanford University Social Media Lab
- Dr Angela Yuson Lee, Stanford University Social Media Lab
- Dr Y. Anthony Chen, Stanford University Social Media Lab
- Zacariah Smith-Russack, Stanford University Social Media Lab

Members of the Academic Advisory Group

- Distinguished Professor Bronwyn Carlson, Head of Critical Indigenous Studies, Macquarie University
- Professor Peter Etchells, School of Psychology, Bath Spa University
- Professor Katherine Keyes, Mailman School of Public Health, Columbia University
- Distinguished Professor Mitch Prinstein, Co-Director of the Winston Center for Technology and the Developing Mind, University of North Carolina, and Chief Science Officer, American Psychological Association.
- Professor Jo Robinson, Professorial Fellow and Director, Centre for Youth Mental Health, University of Melbourne
- Professor Susan Sawyer, Chair of Adolescent Health, University of Melbourne, and Director, Centre for Adolescent Health, Royal Children's Hospital
- Professor Julian Sefton-Green, School of Education, Deakin University
- Associate Professor Aliza Werner-Seidler, Black Dog Institute, University of New South Wales
- Professor Amanda Third, Professorial Research Fellow and Co-Director, Young and Resilient Research Centre, Western Sydney University
- Associate Professor, Munmun De Choudhury, Director of Social Dynamics and Well-Being Laboratory, and Co-Lead of Children's Healthcare of Atlanta Pediatric Technology Center, Georgia Institute of Technology
- Professor Amy Orben, Programme Leader Track Scientist at the MRC Cognition and Brain Sciences Unit, University of Cambridge

2026 - 2027 Budget Estimates

Environment and Communications

Lead/Support contact: Sarah Vandenbroek / Andrew Hyles

SB26-000061

SUBJECT: Digital Duty of Care

Key Deliverables

- On 13 November 2024, the Australian Government announced a commitment to legislate a Digital Duty of Care for online services operating in Australia.
- This was a key recommendation of the independent statutory review of the *Online Safety Act 2021* (the Act).
- The government's response to the review was released on 14 April 2026.
- Between November 2025 and January 2026, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts conducted public and targeted consultation on the Digital Duty of Care.
- This consultation has informed the development of the model, and work is underway to legislate a Digital Duty of Care.

Talking Points

- On 14 April 2026, the government released a response to the independent statutory review of the *Online Safety Act 2021*.
  - The response reiterates the government's commitment to ensuring Australia's online safety laws remain fit for purpose (refer SB26-000062).
- The government is prioritising reforms to legislate a Digital Duty of Care, a key recommendation of the review.
  - Timing of this legislation is a matter for government. The government is committed to introducing the legislation as soon as possible, consistent with the government's legislative priorities.
- A Digital Duty of Care will place legal obligations on services operating in Australia to exercise due diligence and take reasonable steps to prevent reasonably foreseeable harms on their services.
  - This approach emphasises preventing rather than responding to harms.
- The Digital Duty of Care will provide protections for all Australians, with priority given to harms to young people, illegal content and activity, and serious harms arising from platform features, such as AI and recommender systems.
- A Digital Duty of Care will support broad, risk-based and proportionate regulation of all digital service providers and provide a legislative framework that can better accommodate changes in technologies and services in the future.
- A Digital Duty of Care is a significant reform and the development of the model has been informed by consultation with stakeholders and feedback from the community.

Contact: Andrew Hyles **Cleared by:** Sarah Vandenbroek, First Assistant Secretary

Phone: (02) 6136 6187 **Version Number:** 01 **Date:** 25/05/2026

- Careful consideration is being given to appropriate transitional arrangements for industry and eSafety.

Key Issues

- The details of how the Digital Duty of Care will operate remain subject to the legislative drafting process.
- The duty will be designed to accommodate future changes in technology and services.
- The duty is intended to apply to all entities currently regulated by the *Online Safety Act 2021* (the Act) noting that the obligations will be risk-based and proportionate.
  - Entities currently regulated under the Act include:
    - Social media services
    - Relevant electronic services (such as gaming platforms)
    - Designated internet services (such as websites)
    - Gatekeeper services (such as search engine services and app distribution services)
    - Hosting services
    - Internet Service Providers
    - Equipment and operating system services.
- The duty will broadly align with the existing footprint of the Act – focusing on psychosocial harms.
- In drafting amendments to the Act, a key principle will be to ensure the duty of care creates an effective, simplified framework which operates coherently with related initiatives, including proposed reforms to Australia's privacy laws.
- In implementing the duty, the transparency reporting powers under the Basic Online Safety Expectations (BOSE) will be subsumed into the Digital Duty of Care – making them enforceable.
- The current codes and standards made under Part 9 of the Act will complement the Digital Duty of Care and may be replaced over time, if appropriate.
- The department is working across government and looking internationally to learn from successes and challenges experienced by countries implementing similar online safety laws.
  - The model being considered by Australia will align with the EU approach to a single overarching duty of care rather than the UK approach of multiple duties.
  - The UK approach creates added regulatory complexity and requires a significant amount of guidance material as a result.

Consultation

- Consultation is ongoing to inform the design of the Digital Duty of Care and make sure it is appropriate to the Australian context.
- In late 2025, the department conducted a public survey, which received 1,348 responses, and the department also undertook a series of meetings with industry, community and youth representative groups. A summary of these consultation activities is at **Attachment A**.
- The department has engaged with officials in the UK, EU, US, Canada and other countries on their experiences and lessons learned from implementing online safety reforms.

Other views and proposals relating to a Digital Duty of Care

- The Joint Select Committee (JSC) on Social Media and Australian Society released its final report on 18 November 2024. Among other things, the JSC recommended introducing an overarching Duty of Care on online services involving risk assessment and mitigation.
- On 25 November 2024, then independent MP, Ms Zoe Daniel, introduced the Online Safety Amendment (Digital Duty of Care) Bill 2024 in the House of Representatives.
- On 27 November 2024, Senator Hanson Young proposed amending the Social Media Minimum Age Bill to include a number of additional provisions including the imposition of duty of care obligations on large providers.
- In September 2025, Senator Fatima Payman moved Order for the Production of Documents No. 169, regarding correspondence between the Minister for Communications and the department or eSafety Commissioner relating to preparations for a legislated Digital Duty of Care.
- On 1 April 2026, Senator Hanson Young introduced a bill proposing a Digital Duty of Care, which targeted social media algorithms.
- Minister Wells has publicly reiterated the government's intention to consult on, or to introduce, a Digital Duty of Care and intention to bring forward legislation this year.

Supporting Information

Recent Ministerial Comments

- "Well, they have all said that they will abide by domestic law and that the eSafety Commissioner has said she expects swift and emphatic progress on that front that we're talking about, the social media minimum age compliance on Tuesday. Companies who wish to transact business on Australian shores must do the right things by Australians. And I guess the other element to this that is coming is the Digital Duty of Care, which is my big piece of work in comms this year that we hope to legislate by the end of the year. That's going to capture anyone who owns a website or an app to not have addictive features and functions. That captures gambling companies, that captures some of the practices that people wanted to see in the recs of this report, and I hope to hand that down this year, and it will be a game changer. But yeah, it is slogging it out day by day to make cultural change in this country, but it's really important." 2 April 2026, ABC News Afternoon Briefing.
- "One of the reasons the Albanese government is committed to implementing a digital duty of care, which we intend to do through the parliament this year, is to address online harms that are affecting Australians. That includes preventing nudify apps and deepfakes generated by AI and also hate online… We just closed the consultation process for that at the end of last year. We are now working through the consultation responses. We intend to work collaboratively with our parliamentarians to try and get this through the parliament by the end of the year…" 5 March 2026, Question Time Hansard Extract.
- "This is why I am also releasing the Albanese Government's full response to the Review into the Online Safety Act. At the heart of our response is a commitment to legislate a Digital Duty of Care. A Digital Duty of Care makes sure that the proactive safety protections that Roblox is introducing become the norm across big tech rather than just the exception. It will also empower eSafety to react twice as fast to child cyberbullying and to adult cyber abuse, compel more transparency for the tech companies to ensure they are keeping kids safe. And we will transition the Act away from industry-led regulation to more robust legislative rules subject to parliamentary scrutiny, so when new harms emerge, we can act quickly." 14 April 2026, Doorstop Transcript.

Attachments

- A: List of roundtables and other consultation meetings on a digital duty of care model

2026 - 2027 Budget Estimates

Environment and Communications

Lead/Support contact: Sarah Vandenbroek / Anthea Fell / Andrew Hyles

SB26-000062

SUBJECT: Online Safety (including OSA Review and Roblox)

Key Deliverables

- The Australian Government issued its response to the independent review of the *Online Safety Act 2021* (OSA) on 14 April 2026. The response agrees to implement or further consider 64 of the 67 recommendations, including to legislate a Digital Duty of Care.
- The government is also taking action to reduce access to 'nudify' apps and undetectable stalking apps through the duty of care.
- In addition, the government will provide eSafety new powers to issue notices to remove 'nudify' apps and websites.
- In relation to online hate, the government is prioritising a systemic uplift in online safety through the Digital Duty of Care.

Talking Points

- The government is implementing recommendations of the independent Online Safety Act review, with work well underway to legislate a Digital Duty of Care for online services (refer SB26-000061).
- The government is prioritising implementing the duty of care framework to uplift safety for Australians online.
- Alongside the duty of care, the government's response to the Online Safety Act review includes complementary reforms that will be taken forward including improving compliance, enforcement and removal notice powers for eSafety.
- Advice from the eSafety Commissioner and the Special Envoy to Combat Antisemitism, in relation to online antisemitism, will feed into the design of the duty of care.
- Following meetings with the Minister for Communications and the Department of Infrastructure, Regional Development, Communications, Sport and the Arts, Roblox announced in April that it would introduce new protections for children on its platform by mid-year.

Key Issues

<u>Government response to the review of the Online Safety Act</u>

- On 13 November 2024, the government announced that it would introduce a Digital Duty of Care (refer SB26-000061).

- On 2 September 2025, the government announced plans to restrict access to 'nudify' apps and undetectable stalking tools as recommended by the review.
- On 14 April 2026, the government released its full response to the review, which agreed to implement or further consider 64 of the 67 recommendations (see **Attachment A**).
- The government response also committed to introduce legislation that will:
  - Provide eSafety with a new bespoke power to issue notices to remove 'nudify' apps and websites.
  - Streamline processes for eSafety removal notices so seriously harmful content can be taken down more quickly.
  - Require online services to have easily accessible and effective internal dispute resolution and complaints mechanisms.
  - Increase the maximum civil penalties in the OSA to a level more proportionate with the potential harm of underlying offences, and other comparable Commonwealth legislation.
- There are only 3 recommendations which are not supported, recognising the need to ensure our approach is practical, workable and consistent with broader legal and international frameworks.

Governance of the eSafety Commissioner

- The government response also committed to further examining arrangements to strengthen the governance of the eSafety Commissioner.
- The operating environment for online safety regulation is becoming increasingly complex.
- In line with the OSA review recommendations, the government is considering options for the eSafety Commissioner structure, including options to transition eSafety to a multi-member regulator.

Online hate/antisemitism

- On 30 October 2025 the minister met with the Special Envoy to Combat Antisemitism (Special Envoy) in relation to online antisemitism.
- On 18 December 2025, the government announced work between the eSafety Commissioner, the Special Envoy and the Minister for Communications, to provide online safety advice to address antisemitism.
- This formed part of the government's announcement to adopt the Special Envoy's Plan to Combat Antisemitism, and wider response to the Bondi terrorist attack.
- Subsequent meetings in relation to this work were held on 20 January 2026 and 12 February 2026.

- The minister received advice from the Special Envoy and the eSafety Commissioner on 19 February 2026 and 24 February 2026 respectively, in relation to online antisemitism.
- The government is prioritising the duty of care to uplift systemic protections against serious harm for Australians online – in relation to both content and activity as well as features.

Nudify and undetectable stalking apps

- On 2 September 2025, the government announced that it would undertake work to restrict access to 'nudify' apps and undetectable stalking tools.
- Consistent with the response to the OSA review, the government is progressing this commitment through the duty of care framework. The framework will place an obligation on services to put in place systems and processes to prevent the risk of reasonably foreseeable serious harms from the use of their services.
- In addition, in relation to nudify tools, the government committed to introduce new powers that allow eSafety to issue notices to remove nudify apps and websites.
- The design of the new power will be a decision for government and we continue to consult stakeholders, including industry, on scope and operation of the new powers.

Roblox

- On 9 February 2026, the minister wrote to Roblox requesting a meeting following reporting of children being groomed by predators and exposed to graphic and gratuitous content on the platform.
    - Roblox's co-founder and CEO, alongside other senior staff, met with the minister in Brisbane on 25 February 2026.
- Following the minister's meeting with Roblox, on 13 April 2026, Roblox announced a suite of safety improvements for under-16s to be rolled out globally from mid-year. These would result in new accounts for young people, designed to provide age-appropriate content and communications.
- The government welcomes the announcement of further safety uplifts for under-16s and considers the measures could provide a high-level of protection to children on Roblox if implemented appropriately.
- The eSafety Commissioner will monitor the effect of these changes and continue to examine Roblox's compliance with its obligations under the Online Safety Act and relevant industry codes and standards.
    - Under these standards, Roblox is required to prevent the creation and dissemination of child sexual exploitation material and restrict access to age-inappropriate content.

- The department, the Classification Board and Roblox have established a working group to support the classification of experiences (user-generated games) across Roblox. This will help parents and children make informed choices about the experiences they engage in, having reference to the Australian classification ratings.

Support to Expand Youth Education about Online Sextortion – SmackTalk

- The government is investing in the online education and literacy of young Australians to prevent online harms from occurring.
- The government committed $450,000 to SmackTalk for a 2-year grant to deliver information sessions about the dangers of online sextortion, to commence in early 2026.
- SmackTalk offers free educational presentations to schools, sporting clubs, and other organisations to deliver this information.
- The grant agreement was signed on 17 April 2026.

Online Safety Tools in Schools – Alannah and Madeline Foundation

- The government committed an additional $6 million to the Alannah and Madeline Foundation (AMF) for a 3-year grant for free tools to teach kids how to be safe, smart and responsible in the digital world.
- The funding will enable continued free access for all Australian schools and allow AMF to explore opportunities for delivery in non-traditional educational environments, such as Youth Justice, TAFE and other specialty institutions.
- Funding for the new AMF grant is scheduled to commence in the 2026-27 financial year. This commitment builds on the $6 million provided to the AMF over 2023-24 to 2025-26 to deliver their digital education program for children and young Australians.

Online safety funding

- The government provides a strong funding base for the eSafety Commissioner.
- In the 2026-27 Budget, the government provided eSafety with an additional $6 million to:
  - Continue the operation of the National Technology Facilitated Abuse Support Service, which includes operating a dedicated phone line and specialist resources to support frontline workers and victim-survivors of tech-facilitated abuse; and
  - Support the continued delivery of bespoke online safety education programs helping parents and families recognise and prevent online harms.
- The government has also strengthened eSafety's funding, by:
  - Quadrupling eSafety's base funding in the 2023-24 Budget, bringing it to $42.5 million each year ongoing and indexed.

- Providing $6.7 million over 4 years in the 2023-24 MYEFO for eSafety to improve its investigation and response capability for referrals of violent and extremist content, and strengthen its technological capability.
- Providing $76.1 million over 4 years in the 2024-25 MYEFO (and $16.9 million per year ongoing from 2028-29) to support the implementation of a social media minimum age.

Online Harms Ministers Meetings

- The Online Harms Ministers Group has met 3 times since 19 October 2023:
  - 19 October 2023, 4 March 2024 and 1 October 2024.
- Further information was provided in the department's response to Committee Question on Notice Number 176 (refer SQ25-002332).

Background

Final report of the Statutory Review of the Online Safety Act

- The majority of the report's 67 recommendations sit under 4 broad themes:
  - Duty of care – including establishing an overarching duty, risk assessment, mitigation and transparency obligations, statutory categories of harm, simplified definitions of online industry sections, regulator-made enforceable codes, and regulator powers to issue reporting notices and to require audits.
  - Supporting individuals – including enhancements to complaints schemes, mandatory improvements to complaints handling, implementing an Ombuds scheme and awareness raising.
  - A stronger, more effective regulator – including stronger penalties and enforcement, investigation and information sharing, fit-for-purpose definitions of class 1 and 2 materials, and clarifying informal powers.
  - Governance – including transitioning to a Commission model, improved internal processes/transparency, increased resourcing for expanded functions and cost recovery.
- Other recommendations relate to miscellaneous matters including:
  - considering options to prohibit 'nudify' and stalking products
  - convening experts (fusion cells) to address "wicked problems" that cannot be addressed through the OSA alone, such as implications of end-to-end encryption for combatting child sexual exploitation and abuse material
  - long term transition to a single digital regulator

Supporting Information

Questions on Notice (QoNs)

- SQ25-002332 – Online Harms Ministers Meetings
- SQ26-000347 – Nudify apps
- SQ26-000076 – Confirmation of SmackTalk Election commitment figures
- SQ26-000435 – Bondi Beach attack on Chanukah by the Sea celebration (eSafety)
- SQ26-000434 – Deepfakes (eSafety)
- SQ26-000171 – Technology-facilitated abuse (eSafety)
- SQ26-000169 – Fix Our Feeds (eSafety)
- SQ26-000168 – Nudify apps (eSafety)

Recent Ministerial Comments

- "The Albanese Government has shown that we will not sit idly by while kids are being exposed to harmful and graphic content on online platforms." Minister for Communications, 13 April 2026, https://minister.infrastructure.gov.au/wells/media-release/roblox-responds-australias-safety-warnings
- "We made it clear to Roblox that something had to be done – and I welcome these steps towards stronger safety measures on their platform for under-16s, not just in Australia, but globally." Minister for Communications, 13 April 2026, https://minister.infrastructure.gov.au/wells/media-release/roblox-responds-australias-safety-warnings

Relevant Media Reporting

- "Roblox reveals sweeping changes amid Australian crackdown," David Swan, The Sydney Morning Herald, 13 April 2026 – www.smh.com.au/technology/roblox-reveals-sweeping-changes-amid-australian-crackdown-20260410-p5zmsx.html

Attachments:

- A: Government Response to the Independent Review of the *Online Safety Act 2021*

2026 - 2027 Budget Estimates

Environment and Communications

Lead/Support contact: Sarah Vandenbroek / Anthea Fell

SB26-000063

SUBJECT: Social Media Minimum Age

Key Deliverables

- In November 2024, the *Online Safety Act 2021* was amended to introduce a social media minimum age – requiring age-restricted social media platforms take reasonable steps to prevent Australians under 16 years old from having accounts.
- The obligation commenced on 10 December 2025.
- On 31 March 2026, the eSafety Commissioner released a compliance update, which shows that, as of early March, more than 5 million accounts belonging to under-16s have been deactivated, removed or restricted across major social media platforms.
- The eSafety Commissioner has also identified several compliance concerns and is actively investigating 5 platforms for potential breach of obligations: Facebook, Instagram, Snapchat, TikTok and YouTube.

Talking Points

- The Australian Government is taking world-leading action to reduce online harms experienced by young Australians, including passing historic legislation to delay access to accounts on social media until the age of 16.
  - Age-restricted social media platforms include Facebook, Instagram, Kick, Reddit, Snapchat, Threads, TikTok, Twitch, X and YouTube.
- Delaying access to social media will protect young Australians at a critical stage of their development, giving them 3 more years to build real-world connections and online resilience.
- The eSafety Commissioner's recent compliance report shows that, as of early March 2026, major age-restricted social media platforms had removed or restricted access for more than 5 million under-16 accounts.
- Questions on the compliance report should be directed to eSafety.
- The report highlights the positive impact this has had on many young people, including reports from educators who have witnessed the relief felt by students no longer on social media.
- We have also heard from many parents about how the law has helped them to start a conversation with their kids about the harms of social media and supported them to draw a line in the sand when it comes to access.
- the government is aware that gaps remain in the implementation of the social media minimum age, with many under-16s keeping or regaining access to accounts and inadequate practices by some platforms.

Contact: Anthea Fell **Cleared by:** Sarah Vandenbroek, First Assistant Secretary

Phone: (02) 6136 8883 **Version Number:** 01 **Date:** 25/05/2026

- eSafety is actively investigating potential non-compliance in relation to 5 platforms: Facebook, Instagram, Snapchat, TikTok and YouTube.The government has said from the beginning that the social media minimum age is not about chasing perfection. It is about establishing a new norm for social media use, and that will take time.

Key Issues

Platform compliance and implementation

[Questions on compliance should be directed to e-Safety]

- On 31 March 2026, the eSafety Commissioner released a compliance update, which draws on information provided through information gathering notices, public submissions and other sources.
- Despite some good progress, the compliance report confirms that many young people still have accounts on age restricted platforms.
  - Of parents who said their child had an account on social media platforms prior to 10 December 2025, around 7 in 10 reported that their child still had an account on an age restricted platform following the law coming into effect.
- eSafety has identified 3 compliance concerns:
  - Allowing under-16 users to repeatedly attempt age assurance until they pass
  - Not doing enough to prevent underage users whose accounts have been deactivated from immediately opening a new one
  - Ineffective and inaccessible pathways for parents and others to report underage users.
- eSafety is continuing to assess compliance and has advised they are actively investigating potential non-compliance in relation to 5 platforms: Facebook, Instagram, Snapchat, TikTok and YouTube.
- The Hon Anika Wells MP, Minister for Communications has been clear that she expects any systemic compliance failures will be met with the full force of the law – including fines of up to $49.5 million (Minister media release, 31 March 2026).

Circumvention

[Questions on compliance should be directed to e-Safety]

- The independent Age Assurance Technology Trial shows that platforms have the tools to limit circumvention.
- The eSafety Commissioner's regulatory guidance includes an expectation that platforms proactively consider possible circumvention techniques and implement systems to address them.

- The guidance also encourages platforms to take a layered or 'waterfall' approach to compliance, meaning platforms apply several age assurance methods to increase confidence in age estimates.
  - A waterfall approach also helps mitigate against any errors in facial age estimation, which the trial showed to be slightly higher for those between the ages of 12 and 20.

Migration to other, less regulated services

[Questions about migration patterns should be directed to eSafety, which is monitoring changes and patterns of social media use by under-16s.]

- As expected, there have been some short-term increases in downloads of some emerging apps (particularly around 10 December 2025), but eSafety has not seen any significant migration to non-compliant platforms or other online services that are not subject to the social media minimum age obligation.

<u>New legislative rule</u>

- On 25 March 2026, the minister made a new legislative rule to better target the definition of 'age-restricted social media platform' and ensure the law is as effective as possible.
- The rule provides additional conditions a service must satisfy to be an age-restricted social media platform – defined under the Online Safety Act at section 63C.
- A service is now considered an age-restricted social media platform if it:
  - Meets the existing conditions under the definition, i.e. it:
    - has the sole or significant purpose to enable online social interaction
    - allows end-users to interact with others
    - allows users to post material on the service, and
  - [since new rule] has an account-based recommender feature (algorithm), or
  - has one of the following harmful design features while logged in to an account:
    - endless-feed (infinite scroll)
    - feedback features (such as displaying the number of 'likes' or 'upvotes' that a user receives)
    - time-limited features (such as disappearing 'stories').
- The purpose of the new rule is to make clearer – for the community and for industry – the specific design features the law seeks to address, due to the harms they cause.
- It specifies the types of features posing real risks of harm to young people, particularly through continued and addictive engagement with the platform.

Impact of new rule on scope of capture

- In November 2025, eSafety formally assessed Facebook, Instagram, Kick, Reddit, Snapchat, Threads, TikTok, Twitch, X and YouTube as in scope of the law.
- This has not changed under the making of the new rule, and each of these platforms must comply with the social media minimum age.
- The new rule also has no impact on platforms eSafety previously assessed as out of scope. This includes Discord, GitHub, Google Classroom, LEGO Play, and YouTube Kids.

Privacy

- The legislation incorporates strong protections for personal information:
  - platforms must ringfence and destroy any information collected for the purposes of age assurance.
  - platforms must not use information collected through age assurance methods for any other purpose, unless explicitly agreed by the user.
- The legislation is clear that reasonable alternatives to Digital ID must be offered to users.

Public awareness campaign

- Between 19 October 2025 and 11 April 2026, the government ran a public awareness campaign to support parents, carers and young people under 16 prepare for, and navigate the new law.
- $20.0 million was allocated to the campaign.
- Evaluation of the campaign's deliverables and effectiveness against its objectives has commenced and is expected to be completed by mid-year.

Background

High Court challenges

- There are 2 High Court challenges to the social media minimum age on the grounds that the legislation places an unreasonable burden on the implied right under Australia's constitution to freedom of political communication.

Supporting Information

Questions on Notice (QoNs)

- SQ26-000140, regarding legal advice on social media ban
- SQ26-000087, regarding correspondence about implementation of social media ban

Recent Ministerial Comments

- Minister Wells media release, Tech giants warned – step up on social media laws or face significant fines, 31 March 2026:
  - *This new report from the eSafety Commissioner shows that social media giants seem to be trying to get away with doing the bare minimum – I have serious concerns about their compliance with the law*.
  - https://minister.infrastructure.gov.au/wells/media-release/tech-giants-warned-step-social-media-laws-or-face-significant-fines
- Minister Wells media release, Social media minimum age update targets harmful tools, 25 March 2026:
  - *Creating a minimum age to have a social media account is about giving young Australians a break from the pervasive pull of social media.*
  - *Since Gen Alpha got their first smartphone and their first social media account, they have been connected to an addictive dopamine drip.*
  - *Targeted algorithms, doomscrolling, persistent notifications and toxic popularity metres are stealing their attention for hours every day.*
  - *We're shining a light on these harmful and addictive features being used to target young Australians.*
  - https://minister.infrastructure.gov.au/wells/media-release/social-media-minimum-age-update-targets-harmful-tools

Relevant Media Reporting

- Anika Wells rewrote social media ban days before lodging legal defence, Sam Buckingham Jones, Australian Financial Review, 9 April 2026, https://www.afr.com/companies/media-and-marketing/anika-wells-rewrote-social-media-ban-days-before-lodging-legal-defence-20260409-p5zmko
- Two-thirds of under-16s with accounts on Instagram, Snapchat or TikTok kept access despite ban, Josh Butler, The Guardian, 31 March 2026, https://www.theguardian.com/australia-news/2026/mar/31/meta-tiktok-snapchat-google-under-investigation-australia-social-media-ban
- Fifteen-year-old Noah hasn't been kicked off any social media platforms – he's still fighting Australia's under-16 ban in court, Josh Taylor, The Guardian, 11 April 2026, https://www.theguardian.com/australia-news/2026/apr/11/australia-social-media-ban-under-16-teenager-experience