

OFFICIAL

MS24-002100



Australian Government

**Department of Infrastructure, Transport,
Regional Development, Communications and the Arts**

To: The Hon Michelle Rowland MP, Minister for Communications (for decision)

Subject: Acceptance of Final Report of the Statutory Review of the *Online Safety Act 2021*

Critical Date: Routine

Recommendations:	
1. That you agree to accept the updated report of the Statutory Review of the <i>Online Safety Act 2021</i> , at Attachment A as the final report of the review	Agreed / Not Agreed
2. That you note the information on how the Review has addressed all Terms of Reference at Attachment B and the summary of final edits to the Review report at Attachment C	Noted / Please Discuss
3. That you sign the letter of thanks to the independent reviewer, Ms Delia Rickard PSM at Attachment D	Signed / Not Signed
<p>The Hon Michelle Rowland MP Date:</p> <p>Comments:</p>	

Key Points:

1. This brief seeks your approval to accept as final an updated report on the Statutory Review of the *Online Safety Act 2021* (the Act) at **Attachment A**. Based on the proposed Parliamentary Calendar for 2025, the report will need to be tabled by 6 February 2025. As indicated in **Attachment B**, the review report has addressed all of the Terms of Reference. Further information on the Terms and Conditions of appointment and the work undertaken by the independent reviewer, Ms Delia Rickard PSM, is provided under Additional Information.
2. As foreshadowed by Ms Rickard during your meeting on 1 November 2024, she has sought to make a small number of final improvements to the report after providing it to you on the agreed date of 31 October.

OFFICIAL

OFFICIAL

MS24-002100

The changes, detailed in **Attachment C**, include the clarification of three recommendations and an additional five recommendations, all of which are consistent with the text of the report provided on 31 October. Minor edits have also been made to the report text to improve clarity and consistency, and to make corrections including the insertion of missing citations. These changes do not alter the findings of the review. If you are willing to accept the attached as the final report of the review, please sign the letter to Ms Rickard thanking her for completing the review at **Attachment D**.

3. The Department will brief you separately to seek your approval to publish submissions received as part of the review and will conduct a deep dive with you on 21 November 2024 to discuss next steps, after which we will formally brief you on progressing the Government's response to the review and options for implementation. The department is also preparing a designed version of the report, pending your approval for publication.

Financial impacts:

4. The review is funded from within existing departmental resources.

Legal/Legislative impacts:

5. Implementation of the recommendations would require amendments, primarily to the Act.

Stakeholder Implications:

6. The review's recommendations, if implemented, would have significant implications for the Office of the eSafety Commissioner, online services operating in Australia and for Australians. It will be necessary to conduct further engagement and stakeholders will be eager for release of the review report.

Consultation:

The Office of the eSafety Commissioner, Australian Communications and Media Authority, Attorney General's Department, Department of Industry Science and Resources, Department of Social Services, Department of Education, Department of Health, Department of Home Affairs, National Indigenous Australians Agency, Department of the Prime Minister and Cabinet, Department of Foreign Affairs and Trade, Department of Finance and Treasury were consulted on the draft report.

Media Opportunities:

7. On 31 October 2024, your office issued a media release on receipt of the report. The Department will continue to work with your office on upcoming media opportunities relating to the publication of submissions and of the report, and early endorsement of relevant reforms.

Attachments:

Attachment A: Final Report of the Statutory Review of the *Online Safety Act 2021*

Attachment B: Review Terms of Reference and corresponding report sections

Attachment C: Summary of final edits to the Review report

Attachment D: Letter of thanks to the independent reviewer Ms Delia Rickard PSM

Cleared By: Andrew Irwin

Position: Assistant Secretary

Division: Digital Platforms, Safety and Classification

Ph: s22(1)(a)(ii)

Mob: s22(1)(a)(ii)

Cleared Date: 8 November 2024

Contact Officer: s22(1)(a)(ii)

Section: Online Safety Strategy and Research

Ph: s22(1)(a)(ii)

Mob: s22(1)(a)(ii)

Instructions for MPS: Please call Contact Officer prior to dispatching letter to Ms Rickard.

Do you require a signed hardcopy to be returned: No

Responsible Adviser: s22(1)(a)(ii)

PDMS Distribution List: Jim Betts, James Chisholm, Sarah Vandebroek, Andrew Irwin, s22(1)(a)(ii), s22(1)(a)(ii), s22(1)(a)(ii)

OFFICIAL

OFFICIAL

MS24-002100

Additional Information:

In line with the Terms and Conditions of Appointment, Ms Rickard has been actively engaged in the review process and completed the specified work. This includes input into the Terms of Reference, preparation of the issues paper for public consultation, thorough stakeholder consultation, considering responses to the public submissions process and relevant literature and documents, and preparing the review report provided to you on 31 October 2024.

Ms Rickard held 72 meetings and 7 roundtable discussions with stakeholders from community and civil society groups, industry, law enforcement bodies, Australian and international government agencies and views of all stakeholders in the development of the final report and its recommendations.

Released under the Freedom of Information Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

OFFICIAL

ATTACHMENT B

Statutory Review of the *Online Safety Act 2021* – Terms of Reference and corresponding recommendations and sections of the report

Terms of Reference		Recommendation ¹
1	The overarching objects in section 3 of the Act, including the extent to which the objects and provisions of the Act remain appropriate to achieve the Government’s current online safety policy intent.	Recommendation 1 addresses the objects of the Act and calls for more descriptive objectives, including explicit reference to the best interests of the child (Chapter 3)
2	The operation and effectiveness of the following statutory schemes and whether the regulatory arrangements should be amended:	Recommendations 19, 38 and 40 focus on strengthening the powers of the Commissioner to address harmful content under removal schemes (Chapter 10, sections 10.4, 10.6)
2(a)	cyber-bullying material targeted at an Australian child	Recs 15-16 focus on removing barriers to reporting that arise through the prerequisite reporting to platforms (Chapter 7, sections 7.2, 7.3, 7.4)
2(b)	non-consensual sharing of intimate images	No recommendation specific to the image-based abuse scheme, but non-consensual sharing of intimate images is discussed in the report (Chapter 7, sections 7.2, 7.3, 7.4, Chapter 8, section 8.3, Chapter 9, section 9.4) Recommendation 53 about information disclosure recommends the regulator is permitted to disclose information to schools, parents and carers about image-based abuse (Chapter 11, section 11.4).
2(c)	cyber-abuse material targeted at an Australian adult	Recommendations 15-16 focus on removing barriers to reporting that arise through the prerequisite reporting to platforms. Recommendation 18 proposes lowering the threshold for the adult cyber abuse scheme. Recommendation 20 proposes additional powers for end user accountability regarding adult cyber abuse. (Chapter 7, section 7.2, 7.3, 7.4)
2(d)	the Online Content Scheme, including the restricted access system and the legislative framework governing industry codes and standards	Recommendations 29-32 focus on decoupling the Act from the National Classification Scheme (Chapter 7 section 7.3) Recommendation 37 provides broadened powers under the Online Content Scheme (Chapter 9)
2(e)	material that depicts abhorrent violent conduct	No specific recommendation made, but report explicitly states that no changes are needed to this scheme (Chapter 7 section 7.4)
3	The operation and effectiveness of the Basic Online Safety Expectations (BOSE) regime in the Act.	No specific recommendation made, but report supports introducing a duty of care rather than making the BOSE enforceable and building on transparency reporting requirements under BOSE (Chapter 5 section 5.1 Chapter 6 section 6.1)

¹ Please note, this is not a complete list of recommendations. The recommendations listed are those directly related to items listed in the terms of reference.

ATTACHMENT B

4	Whether additional arrangements are warranted to address online harms not explicitly captured under the existing statutory schemes, including:	Recommendation 14 confirms the legality and legitimacy of informal requests for takedown (Chapter 5, sections 5.2, 5.3, 5.6 Chapter 7 section 7.4, Chapter 8)
4(a)	online hate	Recommendation 21 proposes a definition of online hate material (Chapter 5 Section 5.6, 5.8) Online hate is also addressed implicitly through the duty of care [Recommendation 4] and the establishment of codes addressing specific online harms [Recommendation 9] (Chapter 7 sections 7.4, 7.5)
4(b)	volumetric (pile-on) attacks	Recommendations 23-24 focus on defining and addressing volumetric attacks through eSafety's powers (Chapter 7, section 7.4)
4(c)	technology-facilitated abuse and technology-facilitated gender-based violence	Recommendations 27-28 focus on finding solutions for a broad range of 'wicked problems' including technology-facilitated abuse and gender-based violence (Chapter 8, section 8.1, Chapter 12, section 12.3)
4(d)	online abuse of public figures and those requiring an online presence as part of their employment	No specific recommendation made – addressed through proposed changes to the complaint schemes (through adult cyber abuse and volumetric attacks) and through the duty of care (Chapter 7 section 7.4 Chapter 12 section 12.4)
4(e)	other potential online safety harms raised by a range of emerging technologies, including but not limited to: <ul style="list-style-type: none"> • generative artificial intelligence • immersive technologies • recommender systems • end-to-end encryption, • changes to technology models such as decentralised platforms. 	Recommendations 28 proposes the convening of 'fusion cell's to address 'wicked problems more broadly, including the implications of end-to-end encryption for combatting child sexual exploitation and abuse (Chapter 2, Chapter 4 section 4.5 Chapter 5 sections 5.3, 5.10, Chapter 8 section 8.2)
5	Whether the regulatory arrangements, tools and powers available to the Commissioner should be amended and/or simplified, including through consideration of:	
5(a)	the introduction of a duty of care requirement towards users (similar to the United Kingdom's Online Safety Act 2023 or the primary duty of care under Australia's work health and safety legislation) and how this may interact with existing elements of the Act	Recommendation 4 proposes the introduction of an overarching duty of care (Chapter 5). Recommendations 5-7 and 9-12 address the duty of care model and its scope and operation including through codes, risk assessment and mitigation, transparency reporting requirements and audits. (Chapter 6) Recommendation 13 addresses authorised researcher access to data.

ATTACHMENT B

5(b)	ensuring industry acts in the best interests of the child	<p>Recommendation 1 looks to amend the objects of the Act to include explicit reference to the best interests of the child (Chapter 3)</p> <p>Recommendation 8 addresses the best interests of the child through the duty of care and associated risk assessment and mitigation requirements (Chapter 5, sections 5.1, 5.7)</p>
6	Whether penalties should apply to a broader range of circumstances.	Recommendations 34-36, 39 and 41-45 focus on increased penalties, new enforcement powers and considerations for a future licensing scheme. (Chapter 10)
7	Whether the current information gathering powers, investigative powers, enforcement powers, civil penalties or disclosure of information provisions should be amended.	<p>Recommendations 46-49 and 53 focus on new information gathering and disclosure powers. (Chapter 11)</p> <p><i>[Penalties and disclosure of information provisions are discussed above.]</i></p>
8	The Commissioner's functions and governance arrangements, including:	<p>The Commissioner's functions are comprehensively addressed throughout the report, including in relation to the complaints schemes, governance, penalties, information gathering powers and disclosure of information provisions.</p> <p>Notably, recommendations 55-57 go to continuing support for eSafety's promotion, education and awareness raising functions. (Chapter 12 sections 12.1, 12.3, 12.4, 12.5)</p>
8(a)	the Commissioner's roles and responsibilities under the Act	
8(b)	whether the current functions and powers in the Act are sufficient to allow the Commissioner to carry out their mandate.	
9	Whether the current governance structure and support arrangements for the Commissioner provided by the ACMA are fit for purpose for both the Commissioner and the ACMA.	Recommendations 58-63 address a multi-commissioner model, move to a standalone regulator, internal governance and resourcing considerations (Chapter 13, sections 13.1, 13.2, 13.3, 13.4)
10	Whether it would be appropriate to cost recover from industry for eSafety's regulatory activities.	Recommendation 64 addresses possible cost recovery, Chapter 13 (section 13.5)

ATTACHMENT C

Changes to the Final Report of the Statutory Review of the *Online Safety Act 2021*

Detailed below is a summary of the changes made to the final report of the Statutory Review of the *Online Safety Act 2021* following delivery to the Hon Michelle Rowland MP, Minister for Communications on 31 October 2024.

New recommendations and updates to existing recommendations

Three recommendations have been clarified or corrected and five new recommendations added (total now 68). Four of these reflect recommendations made in the text of the report that had not been called out as specific recommendations. The fifth recommends a daily penalty rate for non-compliance with a required action under the duty of care.

- a) **New recommendation 5:** The harms that should be highlighted for attention in reforms to the Online Safety Act should at a minimum include:
 - Harms to young people, including child sexual exploitation and abuse (including grooming), bullying and problematic internet use.
 - Harms to mental and physical wellbeing, including threats to harm or kill, or attacks based on a person or group of people's protected characteristics, such as sex, gender, sexual orientation, race, ethnicity, disability, age or religion.
 - Instruction or promotion of harmful practices, such as self-harm/suicide, disordered eating and dares that could lead to grievous harm.
 - Threats to national security and social cohesion, such as through promotion of terrorism and abhorrent violent extremist content.
 - Other Illegal content, conduct and activity.
- b) **Clarification in recommendation 7** that 'services used by more than 10 per cent of the Australian population should be automatically part of the highest tier with additional mandatory responsibilities.'
- c) **New recommendation 8:** The best interests of the child should be a primary consideration for online service providers in assessing and mitigating the risks arising from the design and operation of their services, including risks to children who may use the service and risks to children as a result of how the service may be used.
- d) **Correction to recommendation 12** to clarify that eSafety should be able to require services to undertake an audit, rather than setting a default annual requirement.
- e) **New recommendation 14:** For the avoidance of doubt, the legislation should make it clear that informal requests for takedown are legal and legitimate as they lead to quicker results for individuals who are often in severe distress.
- f) **Clarification to recommendation 16:** that the statutory delay to issue a removal notice only applies to child cyber bullying and adult cyber abuse schemes.
- g) **New recommendation 35:** The maximum civil penalty that a court can impose for non-compliance with removal notices should be increased to maximum of \$10 million for companies. (Not previously addressed in the report).
- h) **New recommendation 45:** The Government should consider options for introducing a licensing scheme for major services as a condition for operation. [Separating this recommendation out from the recommendation addressing business disruption powers].

Corrections and clarifications in report text

- a) Minor change to the Acknowledgement of Country to include Elders emerging.
- b) Minor changes to text and grammar to improve clarity and readability.
- c) Addition of three references (references 4, 205, and 215) for data included in the text of the report.
- d) Order of harm terminology amended to ‘mental and physical wellbeing,’ placing greater emphasis on harms to mental wellbeing, consistent with the online experience (pages 8, 19, 22, 44, and 96).
- e) Clarify that codes created under the duty of care are not intended to create ‘safe harbours’ for regulated entities (pages 13, 20, and 50).
- f) Removed Section 6.7 ‘Protecting Information’ which was a very short section containing extraneous information.
- g) Recommendation numbers updated to reflect the changes.
- h) Appendix C: Moved the International Justice Mission meeting from the ‘review roundtable’ summary to ‘meetings with individuals and organisations (consistent with meetings coordinated by other stakeholder groups such as the Australian Christian Lobby and eSafety Youth Council).



The Hon Michelle Rowland MP

**Minister for Communications
Federal Member for Greenway**

MS24-002100

Ms Delia Rickard PSM

s47F

s47F

Dear Ms Rickard

I am writing to acknowledge receipt of your final report of the Statutory Review of the *Online Safety Act 2021* (the Act) and to thank you for your work on the review.

The comprehensive and robust review reflects the complexity and breadth of the online safety landscape.

The findings and recommendations put forward in your report put the Australian Government in good stead to protect Australians through strengthened online safety laws. As you are aware, I have already announced the Government's intention to legislate a Digital Duty of Care, reflecting the importance you placed on this in your review.

I have asked my department to ensure that you are notified of the timing of the report's publication.

I look forward to engaging with you further as the Government seeks to develop any reforms arising from the review.

Yours sincerely

Michelle Rowland MP

/ / 2024

The Hon Michelle Rowland MP
PO Box 6022, Parliament House Canberra
Suite 101C, 130 Main Street, Blacktown NSW 2148 | (02) 9671 4780

Released under the Freedom of Information Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

ONLINE SAFETY REFORMS - A DUTY OF CARE

Issue: *Online services are not doing enough to prevent Australians from being harmed online.*

Headline Talking Points:

- *The Albanese Government is committed to legislating a digital duty of care model, to put the onus on industry to prevent online harms at a systemic level.*
- *A systems-based approach, alongside important complaint and takedown schemes, will ensure Australia remains world leading in online safety regulation.*

Key points

- Online interactions have brought many advantages to Australians and are part of our everyday lives. But Australians continue to experience serious harms online.
- Online services are simply not doing enough to prevent Australians from being harmed online.
- This is why the Albanese Government is committing to legislate a **digital Duty of Care** for online services operating in Australia.
- It is time to shift away from reacting to harms and move towards **systems-based prevention**, to stop the harms occurring in the first place.
- A duty of care will require the online industry to take reasonable steps to prevent foreseeable harms.

Last edited: 26/11/2024

SES Cleared by: Sarah Vandenbroek

SES cleared on: 26/11/2024

QB24-000162

ONLINE SAFETY

- A duty of care will require online services to **design their systems with safety at the forefront**, and to quickly identify and remediate any problems when they emerge.
- We understand the pace at which technology and online services change and evolve. A duty of care does not mean services can ‘set and forget.’ This model will require online services to undertake **ongoing risk assessment and management** to ensure their services remain safe for all Australians.
- A duty of care model will build on the existing strengths of the Online Safety Act. These include eSafety’s take down powers and their ability to request transparency reports from industry on what actions they are taking to keep users safe.
- It will also bring Australia into line with international efforts to move towards systems-based regulation, such as in the United Kingdom and European Union.
- A duty of care will complement the Government’s decision to legislate a minimum age of 16 for access to social media and head towards a safer and healthier online ecosystem.

If asked on penalties or enforcement

- Where platforms seriously breach their duty of care we will ensure the regulator can draw on strong penalty arrangements.

Last edited: 26/11/2024

SES Cleared by: Sarah Vandenbroek

SES cleared on: 26/11/2024

QB24-000162

ONLINE SAFETY

Related topics*Response to Review of the Online Safety Act 2021*

- Last month I was pleased to receive Delia Rickard's review of the *Online Safety Act*.
- We are working through this comprehensive report, which made 67 recommendations.
- A response will be provided after the report has been carefully considered. We want to make sure that the reforms we take forward are effective and deliver the best outcomes for Australians.
- One message that stood out in the report is that a duty of care is fundamental.
- Conceptually, this draws on duties of care embedded in our work, health and safety regimes. It is a proven, workable and flexible model.

Implementation

- The Government will work carefully but promptly to develop a duty of care model that can be adopted in Australia.
- The shift towards a duty of care will be a fundamental change to our online safety regulatory framework.

QB24-000162

ONLINE SAFETY

- Though we are clear that this is the right approach, the design and implementation of an appropriate framework will need careful consideration, including transitional arrangements for industry and eSafety.

Released under the Freedom of Information Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Last edited: 26/11/2024
SES Cleared by: Sarah Vandebroek
SES cleared on: 26/11/2024

Background

Online Safety Act Review

- In November last year, I announced the appointment of Ms Delia Rickard PSM, former deputy chair of the Australian Competition and Consumer Commission, to lead a comprehensive independent review of the Online Safety Act.
- The Government brought forward the statutory review by one year to ensure the eSafety Commissioner has the right powers to keep Australians safe in a rapidly evolving online world.
- Ms Rickard completed a thorough examination of Australia’s existing online safety laws, met with more than 100 stakeholders, hosted seven themed roundtables, and received more than 2,200 public consultation responses.
- The review considered:
 - Current provisions in the Act and whether additional protections are needed to combat online harms, including new harms from emerging technologies such as generative artificial intelligence, end-to-end encryption and algorithms
 - The operation and effectiveness of investigation and enforcement arrangements, complaint schemes and approaches for assisting individuals who have experienced online harms
 - The Commissioner’s functions and governance arrangements;
 - Introducing a more systems-based and preventative approaches to online safety regulation, such as a duty of care for users, as adopted overseas.
- On 31 October, I received Ms Rickard’s final report of the review. The report acknowledges the difficult and challenging work undertaken by the Commissioner, and the need for further reforms to ensure our online safety laws keep pace with changes in the online environment.
- The Government will consider the extensive recommendations made by Ms Rickard and respond in due course.

Key Media

Media	Summary
Greens welcome digital duty of care. Call for release of Online Safety Act Review, Media Release (14 November 2024)	The Australian Greens support an EU-style duty of care and are calling for the immediate release of the report of the Online Safety Act Review.
Digital ‘duty of care’ for tech titans, The Australian, Rosie Lewis (14 November 2024)	Summary of announcement of digital duty of care on 13 November 2024.
Platforms must bear harm duty, Australian Financial Review, Sam Buckingham-Jones (14 November 2024)	Summary of announcement of digital duty of care on 13 November 2024, including examples of what a duty of care might mean in practice.
“Safer online spaces for all” – Human Rights Law Centre calls for	The HRLC recommends the Albanese Government implement a regulatory regime similar to the EU’s Digital Services Act, centred on duty of care, risk

Last edited: 26/11/2024

SES Cleared by: Sarah Vandenbroek

SES cleared on: 26/11/2024

QB24-000162

ONLINE SAFETY

more online regulation , LSJ Online , Francisco Silva (8 August 2024)	assessment, risk mitigation, and transparency and accountability measures.
Facebook whistleblower Frances Haugen says Australia has a 'once-in-a-decade chance' to fix its social media law , ABC, Ange Lavoipierre (7 August 2024)	Australia has a "once-in-a-decade opportunity" to regulate social media and should look to the EU's DSA as a north star for online safety regulation, as it focuses upstream, at the source of online harms, rather than at the harms themselves.
How getting big tech platforms to care for their users could mean a better online experience for everyone , ABC, Esther Linder (8 October 2024)	Experts from the Human Rights Law Centre and Reset.Tech Australia endorse the introduction of a duty of care obligation, providing insights into how a duty of care model might work in Australia.

Online Safety - Overarching

Issue: *The online world continues to present new and emerging risks to Australian's safety.*

Headline talking points:

- *We are committed to holding big tech to account for their responsibility to keep Australians safe in the online environments where they interact and connect.*
- *The Albanese Government is addressing online safety risks and harms, and is working in a methodical way to strengthen our legislative regimes.*

Key Points

- The Government is committed to ensuring eSafety has the resources it needs to keep Australians safe online. In the **2023-24 Budget**, the Government quadrupled eSafety's base funding, bringing it to **\$42.5 million** each year with funding ongoing and indexed.
- We also committed **\$7.9 million in the 2024-2025 Budget** to support online safety including:
 - **\$6.5 million in 2024-25** to develop a trial of age assurance technologies to protect children from harmful online content
 - **\$1.4 million over two years (2024-25 to 2025-26)** to boost eSafety's legal and compliance functions.
- To ensure the Online Safety Act is fit for purpose, the Government brought forward the independent **review of the *Online Safety Act 2021***. The review

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(1)

s22(1)

SES cleared on: 25/11/2024

QB24-000079

ONLINE SAFETY

was provided to Government on 31 October. The Government will carefully consider the report and respond in due course.

- The Government established the **Joint Committee on Social Media and Australian Society** to inquire and report on the influence and impacts of social media on Australians. The Committee released its final report on 18 November 2024. The Government will carefully consider the report and respond in due course.

Government policy intent / commitment

- Keeping Australians safe online is, and always will be, a top priority for the Australian Government.
- The Government is taking decisive action to minimise online harms to better protect – not isolate – young people.
- Work to keep our online world safe is ongoing and our Government will continue to hold industry to account and put the safety of Australians first.
- In addition to the measures the Government is already progressing to enhance online safety, the Government has also announced that it will be legislating a digital Duty of Care. The duty of care will require the online industry to take reasonable steps to prevent foreseeable harms.

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(1)

s22(1)

SES cleared on: 25/11/2024

2

QB24-000079

ONLINE SAFETY

Regulation

- The Government has introduced the Online Safety (Social Media Minimum Age) Bill 2024 to enforce a minimum age of 16 for access to social media.
- The Bill also includes stronger penalties of up to \$50 million for online safety breaches. This will apply to digital platforms for systemic breaches of the minimum age requirement, and for breaches of enforceable industry codes and standards under Part 9 of the *Online Safety Act 2021*.
- To ensure the *Online Safety Act 2021* keeps pace with the evolving digital environment, the Government has strengthened the Basic Online Safety Expectations (BOSE) Determination.
- The changes include new expectations requiring industry to consider user safety in the design and implementation of **generative AI capabilities and recommender systems**. The changes also require that the **best interests of the child** be a primary consideration in the design and operation of any service likely to be used by children.
- These changes clearly highlight the Government's expectations of industry and its responsibility to keep Australians, particularly children and young people, safe online.
- Amendments to strengthen the BOSE Determination also go hand in hand with the important work the eSafety Commissioner and industry are doing

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(1)

s22(1)

SES cleared on: 25/11/2024

3

QB24-000079

ONLINE SAFETY

to develop codes addressing illegal and restricted content online. Industry is developing the second phase of codes, which will protect children from online pornography.

- The Government's age assurance trial will complement the work eSafety is doing on Phase 2 Codes.

Social Media: digital and media literacy

- The eSafety Commissioner provides resources and advice on managing screen time and taking care of mental health while on social media.
 - This includes a wealth of practical support for parents, teachers and kids, including free guides on how to use parental controls, and how parents can talk to kids about topics like cyberbullying, mental health, and pornography, in an age-appropriate way.
- In the October 2022 Budget, the Government provided **\$6 million over three years** to the Alannah and Madeline Foundation to deliver its digital and media literacy education products free in Australian schools.
 - This funding also supported the development and implementation of a new eSmart Digital Licence for lower primary school.

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(1)

s22(1)

SES cleared on: 25/11/2024

4

QB24-000079

ONLINE SAFETY

Related topics

- The Government is supporting work to improve **online dating** safety, conducting a trial of **age assurance** technologies and commencing a review of **classification reforms**.
- The Government is also addressing issues of **gender-based violence, sextortion and hate-speech and doxing**.
- The Government has also commenced the fifth phase of the Stop It At the Start campaign to tackle online misogyny and disrespectful behaviour towards women.

Background

Review of the Online Safety Act 2021

- An issues paper to support public consultation was released on 29 April 2024. Submissions closed on 21 June 2024. The final report was provided to Government on 31 October 2024.

eSafety funding

- In the 2024-25 Budget, eSafety was provided with an additional \$1.4 million over two years to support legal and compliance functions under the Act. On 19 October 2024, eSafety was provided with \$6.7 million over four years to improve their capacity to investigate referrals and take action in response to online violent and terrorist content stemming from the Israel-Hamas conflict. In the 2023-24 Budget, eSafety was provided with increased funding. eSafety will receive an additional \$132.1 million over four years and see its base funding increase from \$10.3 million to \$42.5 million each year with funding ongoing and indexed.

Industry codes and standards

- Industry is developing codes under the Online Content Scheme in two phases at the request of the eSafety Commissioner. The first set of codes address the most seriously harmful online content, such as child abuse material and pro-terror content. Six of the eight online industry sections have registered and commenced codes.

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(

s22(1)

SES cleared on: 25/11/2024

5

QB24-000079

ONLINE SAFETY

- The industry standards for relevant electronic services and designated internet services were tabled in Parliament in June 2024. The standards will commence on 22 December 2024.
- On 1 July 2024, the Commissioner issued notices to industry requesting that they develop the second phase of codes which will focus primarily on class 2 material including online pornography. Public consultation on the draft codes developed by industry commenced on 22 October 2024 and closed on 22 November 2024. Industry must provide final draft codes to the Commissioner by 19 December 2024.
- Industry codes and standards impose enforceable obligations on industry. If industry fails to meet a direction from the eSafety Commissioner to comply with an industry code, or fails to comply with an industry standard, they can face civil penalties of up to 500 penalty units (\$825,000 for a corporation).

Reforms to the BOSE Determination

- On 31 May 2024, the new BOSE Determination came into effect.
- On 22 July, eSafety issued periodic reporting notices to industry on the steps they are taking to address child sexual exploitation and abuse on their platforms.
- On 2 September, eSafety requested information under section 20 of the BOSE Determination from selected social media services on the number of children using their services, and their age assurance systems and processes.

Joint Committee on Social Media and Australian Society

- On 21 October 2024, the Joint Committee on Social Media and Australian Society released its second interim report focused on digital platforms and the traditional news media.
- The Committee's final report was released on 18 November 2024. The Committee made 12 recommendations including in relation to the introduction of a duty of care obligation on digital platforms, education support and digital competency, data access for independent researchers, data gathering on the impact of social media on wellbeing, giving users more control of algorithms and recommender systems to manage what they see on social media, and updating Parliament on the outcomes of the age assurance trial.

Key Media

Media	Summary
Give me your passcode (25 November 2024, Herald Sun (Melbourne))	Australian men are twice as likely as women to see possible coercive control red flags, such as tracking a partner via their phone or having access to their passcodes and online accounts as being "reasonable" or "signs of care". Experts say the normalisation of such tech-based control is a form of domestic violence and "known precursor" to intimate partner homicide.

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(

s22(1)

SES cleared on: 25/11/2024

QB24-000079

ONLINE SAFETY

<p>Virtual Insanity (24 November 2024, Sunday Times (Perth))</p>	<p>Parents have been warned about the perils of their children falling in love with virtual girlfriends or boyfriends powered by artificial intelligence. Virtual partner apps are easy to download and excessive engagement could potentially lead to "unhealthy emotional dependencies that can lead to psychological damage".</p>
<p>Armed & Dangerous (24 November 2024, Sunday Herald Sun (Melbourne))</p>	<p>Each day in Victoria at least two children, some as young as 10, are arrested for carrying or assaulting people with dangerous weapons. Police flagged social media as one of the drivers behind young people carrying weapons and committing crimes, such as break-ins and car thefts for online notoriety.</p>
<p>Teenage boys on diets of danger (21 November 2024, Herald Sun (Melbourne))</p>	<p>Teenage boys pictured in school uniforms to promote huge tubs of gym supplements, young TikTok stars lauding "bulk and shred" diets, and extensive marketing of high caffeine pre-workout powders are deeply worrying Australian eating disorder experts.</p>

Last edited: 25/11/2024

SES Cleared by: Sarah Vandenbroek, FAS, Digital Platforms, Safety and Classification Division, s22(1)

s22(1)

SES cleared on: 25/11/2024

7

ONLINE SAFETY – OVERARCHING

Issue: *The online world continues to present new and emerging risks to Australian's safety.*

Headline Talking Points:

- *We are committed to holding big tech to account for their responsibility to keep Australians safe in the online environments where they interact and connect.*
- *The Albanese Government is addressing online safety risks and harms, and is working in a methodical way to strengthen our legislative regimes.*

Key points

- The Government is committed to ensuring that eSafety and other government agencies have the resources they need to keep Australians safe online.
- Following the passage of the Social Media Minimum Age legislation, the Government provided **\$76.1 million over four years from 2024–25** to implement the minimum age of access to social media including:
 - **\$45.7 million over four years from 2024–25 (and \$12.3 million per year ongoing)** for eSafety to provide regulatory oversight and enforcement functions;
 - **\$15.5 million over four years from 2024–25 (and \$3.5 million per year ongoing)** for the Department of Infrastructure, Transport, Regional Development, Communications and the Arts to support the delivery of the Government's online safety priorities; and

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

QB25-000119

ONLINE SAFETY

- **\$5.0 million over four years from 2024–25 (and \$1.1 million per year ongoing)** for the Office of the Australian Information Commissioner to provide regulatory oversight of the privacy safeguards.
- We also committed **\$7.9 million in the 2024-2025 Budget** to support online safety including:
 - **\$6.5 million in 2024-25** to develop a trial of age assurance technologies to protect children from harmful online content
 - **\$1.4 million over two years (2024-25 to 2025-26)** to boost eSafety's legal and compliance functions.
- In the **2023-24 MYEFO**, the Government provided **\$6.7 million over four years** for eSafety to enable a more comprehensive investigation and response capability for referrals of violent and extremist content, and to improve eSafety's technological capability.
- All this was in addition to the **2023-24 Budget** where the Government quadrupled eSafety's base funding, bringing it to **\$42.5 million** each year with funding ongoing and indexed.
- To ensure the Online Safety Act remains fit for purpose, the Government brought forward the independent **review of the *Online Safety Act 2021***.

The review report was provided to Government on 31 October and was tabled on 4 February in accordance with timelines set out in the Act. It

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

2

QB25-000119

ONLINE SAFETY

makes 67 recommendations. Consultation with key stakeholders on the recommendations has commenced.

- The Government will carefully consider the report and respond in due course.
- The Government established the **Joint Committee on Social Media and Australian Society** to inquire and report on the influence and impacts of social media on Australians. The Committee released its final report on 18 November 2024. The Government is carefully considering the report and will respond in due course.

Government policy intent/commitment

- Keeping Australians safe online is, and always will be, a top priority for the Australian Government.
- The Government is taking decisive action to minimise online harms to better protect – not isolate – young people.
- Work to keep our online world safe is ongoing and our Government will continue to hold industry to account and put the safety of Australians first.
- In addition to the measures the Government is already progressing to enhance online safety, the Government has also announced that it will be legislating a digital Duty of Care. The duty of care will require the online industry to take reasonable steps to prevent foreseeable harms.

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

3

QB25-000119

ONLINE SAFETY

Regulation

- The recently enacted *Online Safety (Social Media Minimum Age) Act 2024* enforces a minimum age of 16 for access to social media.
- The Act also includes stronger penalties of up to \$50 million for online safety breaches. This will apply to digital platforms for systemic breaches of the minimum age requirement, and for breaches of enforceable industry codes and standards under Part 9 of the *Online Safety Act 2021*.
- To ensure the *Online Safety Act 2021* keeps pace with the evolving digital environment, the Government has strengthened the Basic Online Safety Expectations (BOSE) Determination.
- The changes include new expectations requiring industry to consider user safety in the design and implementation of **generative AI capabilities and recommender systems**. The changes also require that the **best interests of the child** be a primary consideration in the design and operation of any service likely to be used by children.
- These changes clearly highlight the Government's expectations of industry and its responsibility to keep Australians, particularly children and young people, safe online.
- Amendments to strengthen the BOSE Determination also go hand in hand with the important work the eSafety Commissioner and industry are doing

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

4

QB25-000119

ONLINE SAFETY

to develop codes addressing illegal and restricted content online. Industry is developing the second phase of codes, which will protect children from online pornography.

- The Government's age assurance trial will complement the work eSafety is doing on Phase 2 Codes.

Social Media: digital and media literacy

- The eSafety Commissioner provides resources and advice on managing screen time and taking care of mental health while on social media.
 - This includes a wealth of practical support for parents, teachers and kids, including free guides on how to use parental controls, and how parents can talk to kids about topics like cyberbullying, mental health, and pornography, in an age-appropriate way.
- The Government is committed to empowering children and young people with the skills and confidence they need to stay safe and thrive in the online world.
 - Under the Safe Kids are eSmart Kids program, we committed **\$6 million over three years** to the Alannah and Madeline Foundation to deliver its "eSmart" digital and media literacy education products free in Australian schools.

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

5

QB25-000119

ONLINE SAFETY

- eSmart products provide schools the tools they need to teach kids how to be safe, smart and responsible in the digital world.
- The program includes three products, spanning three age groups:
 - 4 to 9 (**eSmart Digital Licence for lower primary school**),
 - 96 schools engaged, 30,096 students connected
 - 10 to 14 (**eSmart Digital Licence+**) and
 - 548 schools registered, 68,549 students connected
 - 12 to 16 (**eSmart Media Literacy Lab**).
 - 76 schools registered, 5,126 students connected
- The grant covers the period 2023-24 to 2025-26.

Related topics

- The Government is supporting work to improve **online dating** safety, conducting a trial of **age assurance** technologies and commencing a review of **classification reforms**.
- The Government is also addressing issues of **gender-based violence, sextortion and hate-speech and doxing**.
- The Government has also commenced the fifth phase of the Stop It At the Start campaign to tackle online misogyny and disrespectful behaviour towards women.

Last edited: 31/01/2025

SES Cleared by: Sarah Vandebroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

6

Background

Industry codes and standards

- Industry is developing codes under the Online Content Scheme in two phases at the request of the eSafety Commissioner. The first set of codes and standards address the most seriously harmful online content, such as child sexual exploitation material and pro-terror content. These codes and standards have commenced.
- On 1 July 2024, the Commissioner issued notices to industry requesting that they develop the second phase of codes which will focus primarily on class 2 material including online pornography. Public consultation on the draft codes developed by industry commenced on 22 October 2024 and closed on 22 November 2024. Industry must provide final draft codes to the Commissioner for assessment by 28 February 2025.
- Industry codes and standards impose enforceable obligations on industry. If industry fails to meet a direction from the eSafety Commissioner to comply with an industry code, or fails to comply with an industry standard, they can face civil penalties of up to 30,000 penalty units (\$49.5 million for a corporation).

Reforms to the BOSE Determination

- On 31 May 2024, the new BOSE Determination came into effect.
- On 22 July, eSafety issued periodic reporting notices to industry on the steps they are taking to address child sexual exploitation and abuse on their platforms.
- On 2 September, eSafety requested information under section 20 of the BOSE Determination from selected social media services on the number of children using their services, and their age assurance systems and processes.

Key Media

Media	Summary
Twiggy backs ALP's online safety law reforms -The Australian, 5 February 2025	The review has 'recommended a raft of changes that would up-end the Online Safety Act 2021'. Recommendations include increased fines for non-compliance by platforms, transparency requirements including sharing data with authorised researchers, and reduced wait times for actioning of complaints to eSafety. The government has also been urged to consider business disruption powers and the feasibility of requiring online companies to have a local presence. Andrew Forrest said the review was an "important step" and now "was the time for action".
Hit Big Tech where it hurts – Herald Sun, 4 February 2025	Australia needs a bigger stick for tech giants who fail to reduce harms like the spread of child sex material, terrorism content and online hate and recommends increasing fines by billions of dollars, a major review says. In an effort to depoliticise

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

QB25-000119

ONLINE SAFETY

	what constitutes “online hate material” the federal government is also being advised to add a definition to Australia’s Online Safety Act that captures attacks against a person based on a “protected characteristic” such as religion or race, but does not include views regarding “ideas, concepts or institutions”.
Review puts tech giants on notice over online safety – MSN Australia 4 February 2025	A report reviewing online safety laws will be released by Communications Minister Michelle Rowland on Tuesday, after it was provided to the government last October. The review's 67 recommendations include simplifying definitions to online platforms to better reflect safety risks and future proof the legislation and identifying harms to be placed at the forefront of action. It is unlikely the government will respond to the review this fortnight of parliamentary sittings, as it intends to consult with stakeholders.
Government postpones big stick for big tech until after election after billions in fines recommended (ABC News, 3 February 2025)	Plans to toughen online safety requirements for big tech platforms are on ice after the review recommended threatening platforms with billions of dollars in fines for breaches of duty of care. Communications Minister Michelle Rowland has been sitting on the recommendation since November and will publish it on Tuesday without stating the government's position.
Social media giants face massive fines under proposed safety laws – Financial Review, 3 February 2025	Social media giants that fail to adequately protect their Australian users would be hit with multibillion-dollar fines under new rules recommended by a sweeping review of online safety laws. Other recommendations include a ‘world first’ duty of care on social media platforms. This is something Communications Minister Michelle Rowland indicated last November that Labor would pursue in its next term of government.
‘Porn’ comic banned but kids can borrow (the Australian, 22 January 2025)	eSafety has classified a graphic novel as ‘class 2’ material but it is still available for children to access in public libraries. The Australian Classification Board <u>has not</u> evaluated the print version of the graphic novel.

Last edited: 31/01/2025

SES Cleared by: Sarah Vandenbroek,

FAS, Digital Platforms, Safety and Classification Division, s22(1)(a)(ii)

SES cleared on: 31/01/2025

8



Australian Government

Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

Review of the Online Safety Act 2021

Deep Dive with Minister Rowland

Presented by Sarah Vandebroek, Andrew Irwin and s22(1)(a)(ii)

29 November 2024

Overview

- Discuss key areas of reform proposed by the Review of the *Online Safety Act 2021*
 - *Theme 1: Duty of care*
 - *Theme 2: Supporting individuals*
 - *Theme 3: A stronger, more effective regulator*
 - *Theme 4: Governance*
 - *Theme 5: Other*

s47C



Review recommendations – at a glance

Workstream	Number of Recs	Minister’s portfolio remit	Recs requiring legislation
Duty of Care	12	11	11*
Supporting individuals	15	12	11*
A stronger and more effective regulator	23	23	23
Governance	7	5	4
Other	10	4	3*



Note: * final number may change following further consideration
 Review of the Online Safety Act 2021: Next Steps

Theme 1: Duty of Care

Proposal: make industry take responsibility for improving safety on their services by establishing a strong systemic and preventative approach to regulating online harms.

Rationale: the Act currently provides limited systemic and enforceable regulation through codes. eSafety is forced to employ a reactive ‘whack-a-mole’ approach to online harms. Aligning with international counterparts is expected to improve platform compliance.

Review Recommendations:

- Establish an overarching duty of care and statutory categories of harm
- Simplify definitions of online industry sections
- Apply the duty to online industry sections, with regulatory power to designate services as having ‘high reach’ or ‘high risk’
- Require high ‘reach or risk’ platforms to conduct risk assessments, produce transparency reports, resource internal compliance and share data with authorised researchers
- Empower the regulator to issue enforceable codes, require responses to reporting notices and require independent audits

Implementation risks: managing transition to new regulatory arrangements, balancing obligations and burden, securing resources for the regulator, challenges in enforcing regime on overseas entities.

Key components proposed for a Duty of Care

A singular and overarching duty of care would create a legal duty for online service providers **to take reasonable steps to address and prevent foreseeable harms on their services.**

The principal components of the duty would include:

1. Statutory **categories of harm** to define the scope of the duty
2. Application of the duty to broad **categories of the online industry**, with regulatory power to designate services as having high reach or risk
3. An obligation for high reach or risk platforms to conduct regular **risk assessments** and produce regular **transparency reports**
4. Regulatory powers to issue **enforceable codes** for services, to require responses to **reporting notices** and to require high reach or risk services to conduct **independent audits**

Duty of care – implementation timelines

s47C



Released under the Freedom of Information Act 1982 by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Theme 2: Supporting Individuals

Proposal: Strengthen, and improve access to, complaint schemes to improve the safety net for Australians online when harmful material is posted.

Rationale: Poor user awareness of complaint schemes, schemes too complicated, adult cyber abuse threshold too high, regulator has limited ability to address harmful patterns of conduct (volumetric attacks, online hate, repeat abuse, reposting).

Review Recommendations:

- **Increase awareness** - through simple and targeted communications
- **Simplify complaint schemes** - reduce reporting barriers, increase consistency of available regulatory responses, add new powers to address reposting, harmful posting, and volumetric attacks
- **Broaden the adult cyber scheme** - lower the threshold, consider online hate and volumetric attacks
- **Broader support** for Australian's experiencing online harms - complaint processes, no wrong door, digital ombuds scheme

Implementation risks: defining online hate and volumetric attacks, balancing human rights, increased demand on regulatory resources, privacy risks (no wrong door).

Theme 3: A stronger, more effective regulator

Proposal: To strengthen and remove barriers to the effective operation of the regulator.

Rationale: Penalties are insufficient to act as effective tools of enforcement alone and removal powers are impeded by unnecessary conditions. If the regulator's powers are unduly limited it could hinder investigations and the opportunity for cooperation with other online safety bodies (e.g. ACCCE) to improve outcomes. Links between the Online Content Scheme and the National Classification Scheme are no longer fit for purpose.

Review Recommendations:

- Clarify informal powers
- Enhance penalties and enforcement powers
- Create fit-for-purpose definitions of class 1 and class 2 material
- Enhance investigation and information sharing powers

Implementation risks: Definitional complexity (class 1 and class 2 material, user generated content), privacy concerns and balancing human rights (obtaining end-user information).

Theme 4: Governance

Proposal: to enable collective decision-making, and promote independence and transparency.

Rationale: A complex operating environment makes decision-making more difficult and contested, and is subject to public scrutiny. Improved transparency can improve public confidence in and awareness of the regulator.

Review Recommendations:

- **New governance model** - comprised initially of a Chair, Deputy Chair and one other commissioner
- **Strong internal governance** - to improve transparency of the Commission
- **Transition to a standalone, independent Online Safety Commission**
- **Appropriately resource eSafety** - including a cost recovery mechanism

Implementation risks: There are risks and complexities in changing eSafety's governance, either moving to a Commission model within the ACMA or separating into an independent entity. Cost recovery would be complex and potentially impact other entities regulating digital platforms.

Theme 5: Other Recommendations that fall outside the four reform workstreams

Review Recommendations:

- **Minimise gaps and fragmentation in online harms regulation**
 - *consider recognising role of online safety related services and technology in detecting CSAM (offence exemption)*
 - *consider options to prevent access to ‘nudify’ or undetectable stalking apps*
 - *consider central online harms regulator (whole of Government reform)*
- **Facilitate stakeholder collaboration to solve ‘wicked’ issues**
 - *enable Government and regulator to form ‘fusion cells’*
- **Minimise enforcement issues for offshore service providers**
 - *require contact point for greatest reach and risk services*
 - *consider requiring local presence, consider licensing services (potential risk: Free Trade Agreement interactions)*
- **Optimise sequencing and review of proposed reforms**
 - *prioritise duty of care, Commission regulator model (with rebranding), and increased resourcing*
 - *a future statutory review*

s47C



Infrastructure, Transport, Regional Development, Communications and the Arts