Inquiry into the Internet Search Engine Services Online Safety Code

September 2025

Australian Government | eSafetyCommissioner

eSafety.gov.au

Contents

Introduction

The eSafety Commissioner (eSafety) welcomes the opportunity to make a submission to the Environment and Communications References Committee's *Internet Search Engine Services Online Safety Code* inquiry.

eSafety is Australia's independent regulator, educator and coordinator for online safety. Our purpose is to help safeguard Australians from online harms and to promote safer, more positive online experiences.

Given the focus of the inquiry, our submission will concentrate on regulatory measures aimed at protecting children and young people online. To contextualise our submission, we first provide an overview of eSafety's remit, role and approach in general terms, before then providing more specific responses to the Terms of Reference.

eSafety's role and functions

We make the following observations in relation to our regulatory approach.

- eSafety's remit is set out in the *Online Safety Act 2021* (Online Safety Act), specifically the eSafety's Commissioner's powers and functions.[1] We perform our functions and powers in accordance with our legislated remit.
- eSafety is an independent statutory office. Once laws are passed by the Australian Parliament, our role is to implement and enforce laws, namely the Online Safety Act.
- Like many other Commissioner roles within Australia, the role of the eSafety Commissioner is not an elected one. It is a statutory appointment by the Minister of Communications. The Online Safety Act sets out the criteria that the Minister must be satisfied of to appoint someone to the role of eSafety Commissioner, which is that the person appointed has substantial experience or knowledge and significant standing in a certain field.[2]
- eSafety has demonstrated its ability to protect Australians and hold online services to account through a regulatory approach that is risk-based, harm-based, balanced, fair and proportionate.

[1] Sections 27 and 28 of the Act.
[2] Section 167 of the Act.

- eSafety administers a range of regulatory regimes under different arrangements. This includes:
    - Regimes where eSafety is the sole regulator, such as our complaints-based schemes. We were designed to serve as a safety net for Australians when their reports or calls for help were not addressed by social media platforms. We act as an intermediary to address the power imbalance between the individual and online service to remediate online harm.
    - Regimes where eSafety is a joint regulator, such as in the context of the Social Media Minimum Age (SMMA) obligation, where we share regulatory responsibilities with the Office of the Australian Information Commissioner (OAIC). We work collaboratively to ensure safety and privacy obligations are upheld.
    - Regimes where there are co-regulatory measures, such as industry codes and standards, where we work with industry. We note that in line with our respective responsibilities, it is the responsibility of industry to create codes and to consult with eSafety. eSafety's does not draft codes: rather, our responsibility is to assess whether they meet the statutory requirements for registration and, if so, register and enforce them. The threshold set in the Online Safety Act is whether or not the eSafety Commissioner believes the industry codes meet 'appropriate community safeguards'. Where eSafety is not satisfied the draft codes meet the statutory requirements, eSafety may determine an industry standard. Standards are disallowable instruments that are subject to Parliamentary scrutiny. We explore the codes and standards framework in more detail later in this submission.
- eSafety is subject to a range of accountability and transparency measures. This includes:
    - Fulfilling a range of reporting, governance and compliance arrangements. This includes corporate and annual reporting requirements, as well as requests under the *Freedom of Information Act 1987*.
    - Providing a range of review processes for our reviewable decisions. In addition to internal review processes, eSafety decisions are also reviewable by the Administrative Review Tribunal, the Federal Court of Australia and the Commonwealth Ombudsman.
    - Appearing at Senate Estimates hearings and respond to information requests by the Australian Parliament.

- eSafety also promotes accountability and transparency in our work. This includes:
    - Publishing regulatory guidance for each of our schemes, as well as broader compliance and enforcement materials. These outline how we apply our regulatory functions and powers in a flexible and integrated way to promote compliance and achieve good outcomes for all Australians.
    - Undertaking deep consultation, engaging with a wide variety of stakeholders and pursuing an extensive array of communication and awareness raising initiatives. These are published on our website to promote transparency and accountability of eSafety's work, while also seeking to raise the profile of online safety.
    - Participating in inquiry and review processes, both within Parliament and across the federal, state and territory level, and publishing our submissions. This ensures a nationally coordinated approach to online safety within Australia that leverages respective competencies across the jurisdictions.
- eSafety's remit under the Online Safety Act has expanded since our establishment in 2015. All the expansions listed below have occurred through laws passed by the Australian Parliament. Of note:
    - In 2015, eSafety was established as the Office of the Children's eSafety Commissioner through the *Enhancing Online Safety Act 2015*.
    - In 2017, eSafety's remit was expanded to include all Australians, which resulted in the name change from Children's eSafety Commissioner to eSafety Commissioner.
    - In 2019, eSafety's remit was expanded to include additional responsibilities under laws criminalising the sharing of Abhorrent Violent Material, such as terrorist or extreme violent content.
    - In 2021, eSafety's remit was more systematically and comprehensively expanded through the *Online Safety Act 2021.*
- As with all other Bills or legislative instruments, these legislated changes included a Statement of Compatibility, which assessed the compatibility of the measures with the rights and freedoms recognised in the seven core international human rights treaties that Australia has ratified. Each time, the measures have been assessed as compatible.
- eSafety's legislative framework has been independently reviewed twice during our 10 years of operation. Both reviews positively affirmed the vital role eSafety plays in

keeping Australians safer online, while also supporting measures to strengthen our legislative framework. The most recent review was conducted by Delia Rickard PSM and the final report completed in October 2024. One of the key recommendations was the introduction of a duty of care under the Online Safety Act, which the Government has agreed to. This will build upon eSafety's work driving systemic reform to date. It will ensure the onus of safety is on industry, rather the individual, while strengthening eSafety's ability to hold online services to account.

eSafety's approach

As Australia's online safety regulator, we have a broad remit with a range of regulatory levers under the Online Safety Act. We take a risk and harms-based approach to our work, which means we aim to minimise harm and do that in a way that is balanced, fair and proportionate to risk.

Our regulatory approach is underpinned by three pillars:

- Prevention: While eSafety acts as an important safety net for Australians online, our primary goal is to prevent online harms from happening in the first place. This work falls under our prevention pillar.
- Protection: Where online harm does occur, eSafety offers tangible, rapid assistance. This work falls under our protection pillar.
- Proactive and systemic change: With the rapid evolution of technology, eSafety knows we need to be at the forefront of anticipating, mitigating and responding to online harms. This work falls under our proactive and systemic change pillar.

These pillars reflect our broad and holistic remit. The way the pillars work together reflects how eSafety's various functions work together to create a multidimensional regulatory toolkit.

Similarly, eSafety supports a layered approach to online safety across the tech stack. This is about ensuring multiple, reinforcing protections that mitigate against a single point of failure and ensure responsibility is distributed across the tech stack. It is also about ensuring the onus of responsibility for safety does not fall on the individual.

Combatting online harm is a global challenge. We therefore work as part of a cross-sector and multijurisdictional online safety ecosystem to share information and insights, which support regulatory coherence and reduce unnecessary burdens on industry. We also seek to promote and embed digital literacy and capacity building across the entire community.

eSafety recognises that online safety requires a whole of community approach. We also recognise the diversity of individuals and that individuals will engage with digital technology in ways that reflect their circumstances and experiences. We focus and draw upon an individual's abilities, knowledge and capacities in supporting them to engage safely online.

We engage with and ensure the voices and perspectives of all Australians inform our work. We ensure this includes the voices and perspectives of First Nations people, people who are LGBTQI+, people with disability and people from culturally and linguistically diverse backgrounds, while also accounting for other diversities, such as gender and age.

Particularly in the context of children and young people, eSafety seeks to recognise the autonomy, resilience, diversity and evolving capacity of children and young people. This is consistent with our requirement under the Online Safety Act to have regard to the Convention on the Rights of the Child in line with, and while performing, functions under the Online Safety Act.

We consult with children and young people to actively listen to their views and give due weight to them in the development of our policies, programs and resources. We also engage with the eSafety Youth Council, which is comprised of children and young people aged 13 to 24 years.

Focus of this submission

Given the interconnections between the Terms of Reference and that different arrangements apply for different schemes, eSafety will be addressing the Terms of Reference thematically, rather than individually.

While noting eSafety has a broader range of programs and initiatives aimed at supporting children and young people be safer online, this submission will focus on:

1. Age assurance.
2. Phase 2 industry Codes.
3. The Social Media Minimum Age obligations.

To assist the Committee, this submission also includes:

- A chronology of the development of codes, standards and the social media minimum age restriction scheme (**Attachment A**).
- An explanation of 'class 1 material' and 'class 2 material' (**Attachment B**).
- A summary of age assurance measures across all Phase 2 Codes (**Attachment C**).

Age Assurance

Both Phase 2 industry codes and the SMMA incorporate age assurance to protect children from online harms.

Before outlining eSafety's involvement and approach to age assurance, we want to clarify terminology. The Terms of Reference for this inquiry refer to 'age verification'. In alignment with other regulators, such as Ofcom, the Age Assurance Technology Trial and emerging practices, eSafety's publications and regulatory materials refer to age assurance. This term captures various processes and methods used to determine person's age or age range: namely, age verification, age estimation and age inference. It is important to distinguish between these methods for several reasons, including that these methods offer different risks, benefits and levels of certainty.

Age assurance methods will also depend on a range of other considerations, including:

- The technology underlying the method itself.
- The circumstances in which the method is used.
- How the method is implemented.
- How the systems around it are designed and deployed.

Age assurance is used throughout this submission to refer to the range of methods and approaches available.

We now outline eSafety's involvement and approach to age assurance, in reference to a timeline that also includes relevant milestones of the Australian Government. We have also noted some of the instances where we made public comments on these matters.

In summary eSafety's involvement and approach to age assurance and at a high-level:

- In February 2020, the House of Representatives Standing Committee on Social Policy and Legal Affairs report, 'Protecting the age of innocence', recommended that the Australian Government direct and adequately resource eSafety to develop an roadmap for the implementation of a regime of mandatory age verification for online pornography. This was to also include among other matters, a suitable legislative and regulatory framework and recommendations for complementary measures to ensure a broader, holistic approach to address the risks and harms associated with children's access to pornography. In June 2021, the Government responded in support of this recommendation.

- In March 2023, eSafety presented the Australian Government with a Roadmap for Age Verification. This explored if and how a mandatory age verification mechanism or similar could practically be achieved in Australia. In August 2023, eSafety also published our Background report that includes evidence and in-depth analysis which supports the assertions, findings and recommendations of the roadmap. To inform this work, eSafety:
    - Conducted a public call for evidence. A summary was published on eSafety's website.
    - Held extensive multi-sector consultations with a range of stakeholders. This included domestic and international government departments and agencies, digital and child rights experts, academics, children's safety advocates, sex work and adult industry groups and the tech industry. Summaries of these consultations have been published on eSafety's website.
    - Conducted desktop and primary research, including a survey and focus groups with participants aged 16-18, supported by further discussion with the eSafety Youth Council. This research was published in September 2023:
        - *Accidental, unsolicited and in your face. Young people's encounters with online pornography: a matter of platform responsibility, education and choice*. Overall, the data indicates that online pornography is a prevalent part of young people's online lives, with Australian young people encountering online pornography at high rates from a young age.
            - Three in four (75%) of the young people surveyed had encountered online pornography. Of these, two in five (39%) had encountered it by the age of 13.
            - The findings suggest that while young people who intentionally seek out online pornography may find it pleasurable and interesting, they generally dislike encountering it unintentionally. Among those surveyed who had encountered online pornography, one in three (30%) had first come across such content unintentionally before the age of 13. Young people in our survey reported two key pathways for unintentional exposure:
                - Two in five (40%) first encountered online pornography when it appeared online while they were searching for something else, or visiting a gaming site, or checking their social media feed.

- One in three (34%) first encountered online pornography when it was shared with them by their peers and/or in social networks (e.g. when someone sent it to them, or showed them, or it appeared in a group chat).

- Due to the pervasiveness of pornography in the online worlds of young people, such encounters appear to be becoming normalised. Young people who encounter pornography unintentionally are more likely to ignore this content than to report it or to seek support and help.

- *Questions, doubts and hopes. Young people's attitudes towards age assurance and the age-based restrictions of access to online pornography.* The report outlines young people's attitudes towards the age-based restriction of access to online pornography and age assurance, including but not limited to age assurance tools.

  - The majority of young people in the survey were supportive of age-based restrictions on accessing online pornography. Focus group participants expressed a keen interest in the restriction of pornographic content that could be encountered unintentionally online, particularly by children.

  - Three in five (63%) of young people in the survey expressed concerns around potential privacy and data security impacts. 58% were concerned that people could lie or bypass age assurance systems and 42% were concerned that the systems could be inaccurate or unreliable.

  - Despite these concerns, most young people in the survey (59%) thought pornography-specific services should use age assurance tools to restrict underage access to pornography and a significant minority thought other online services should use them, including dating sites (41%), social media (40%) and search engines (33%).

- Commissioned an independent assessment of available age assurance and online safety technologies. This independent report was published as an appendix to the Background report.

- One of the key recommendations of the Roadmap delivered in March 2023 was to develop, implement and evaluate a pilot ***before*** seeking to prescribe and mandate age assurance technologies for access to online pornography. This included a recommended robust privacy evaluation as part of the testing.

- The Australian Government responded to the Roadmap in August 2023.
- On 1 May 2024, as part of the Budget 2024-25, the Government announced $6.5 million for the Department of Infrastructure, Transport, Regional Development, Communication and the Arts to conduct a pilot of age assurance technology to protect children from harmful content, like pornography and other age-restricted online services.
- In July 2024, eSafety published an issues paper on Age assurance, which considers the role of age assurance in preventing a broader range of online harms to children and creating safer, age-appropriate online experiences. This issues paper reflects eSafety's ongoing consideration of relevant issues and covered industry and regulatory developments from March 2023 to June 2024. This issues paper was published alongside the Phase 2 Codes position paper.
- On 8 November 2024, the Government announced that it would legislate 16 as the minimum age for access to social media.
- On 15 November 2024, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts announced the tender was awarded for the Age Assurance Technology Trial. The scope of the trial included options to prevent access to online pornography by children and young people under the age of 18 and age-limit access to social media platforms for those under 16 years of age.
- In February 2025, eSafety published Behind the Screen: the reality of age assurance and social media access for young Australians. This examined children's and young people's experiences on social media through research with young people and through information received via Basic Online Safety Expectations information requests. The report found that:
    - 80% of Australian children aged 8-12 used one or more social media service in 2024. This suggests that around 1.3 million children aged 8-12 in Australia may have been using social media. This highlighted potential widespread breaches of minimum age policies.
    - 36% of children aged 8-12 who had used social media had their own account, with 77% of those saying they had help to set up their account(s). This help came mostly from parents or carers.
    - Of the platforms eSafety requested information from, most relied solely on someone's truthful self-declaration of their date of birth at the point of account sign-up. No additional age assurance tools were used upfront at this sign-up stage. This means that if a child provided a false date of birth at sign-

up that indicated they were over 13, they were able to create an account and access the service.

  - Some services – TikTok, Twitch, Snapchat and YouTube – used tools to proactively detect users under 13. However, while other services had some tools and technology available, they were not using it to detect underage users.

- On 31 August 2025, the Age Assurance Technology Trial (AATT) report was published. This was one of a number on inputs into eSafety's regulatory guidance.
- On 4 September 2025, eSafety published summaries of consultation sessions conducted between June and August 2025, including, among others, age assurance vendors, children and young people and civil society. These consultation sessions were held to inform eSafety's approach to implementing the SMMA scheme.
- In September, eSafety published the SMMA regulatory guidance, including guidelines on the taking of reasonable steps as required under the SMMA obligation, along with eSafety's statement of commitment to children's rights.

eSafety is committed to contributing to nuanced conversations about the proportionate and safe use of age assurance. Our position has been reflected in the above documents and through our work on related regulatory schemes. We explore these further later in this submission.

In summary, eSafety's position is that determining a user's age can provide a foundation for safer and more age-appropriate online experiences, but it is not a standalone solution.

- No standalone technological measure is completely effective. Once a platform or service knows the age of a user, it also then needs to be proactive in creating safe, age-appropriate experiences, aligned with Safety by Design principles.
- Age assurance can be an important element in online safety, especially for children, but it must be part of a broader set of complementary safety measures to protect the rights of users, including education in digital literacy and capacity building.
- Implementing age assurance measures cannot be set and forget. eSafety expects to see improvements in age assurance technology continue and for providers to improve their approaches over time. This includes where new approaches are more effective, privacy-preserving or decrease the burden on users. eSafety has seen improvements over time in the accuracy of different age assurance methods,[3] as well as

[3] For example of improvements over time, see the accuracy of facial age analysis technology evaluated by the US National Institute of Standards and Technology.

sophistication in responding to privacy, security, accessibility and other concerns. This expectation has been articulated in our Regulatory Guidance for the SMMA.

- eSafety adopts a technology neutral approach to age assurance, as there is no one technology suitable for all end-users, platforms or circumstances. Neither the Codes, SMMA or associated regulatory guidance mandate or recommend specific age assurance technology or products. As discussed further below, the Regulatory Guidance for the SMMA takes a principles-based approach, underpinned by a consideration of fundamental human rights and the best interests and rights of children.
- Different methods and implementation contexts can also have different accessibility or inclusivity challenges. As set out in our Regulatory Guidance for the SMMA, eSafety expects providers to consider the range of existing and prospective Australian users with diversity in appearance, abilities and capacities, and implement systems and safeguards to ensure their methods are accessible and produce outcomes that are inclusive and fair for all users. Our guidance also encourages providers to offer users a choice of a range of age assurance methods – allowing users to opt for the method that they feel best suits them and their circumstances.

To add further context to eSafety's position, we note that:

- Age assurance is an evolving area of the technology industry and is a burgeoning and continually maturing sector. There is ongoing research and development into novel ways to assess age using less or no personal information, interoperable systems, digital wallet integrations and zero-knowledge proof methods that enable users to have control over their information.
- There are many different approaches under the umbrella of age assurance. The risks, benefits, level of certainty and other considerations regarding use of an age assurance method depend on a number of factors. This includes the technology underlying the method itself, the circumstances in which it is used, how it is implemented and how the systems around it are designed and deployed.
- Research shows public awareness is low on the wide range of age assurance methods available and currently in use, as well as their particular considerations. It is important that platforms and services are transparent and clearly communicate key information to their users. This includes what options are available to them, what information is required, how it is stored, protected or deleted and what users can do if the result is wrong.

The AATT report found that age assurance is technically feasible and is already being used in Australia and internationally, in a range of sectors. Our *Behind the Screen* report, as mentioned above, also reflects varied use of proactive age-detection tools by social media

providers. Our Regulatory Guidance for SMMA, as also mentioned above and discussed further below, outlines eSafety's expectations regarding accessibility and inclusivity challenges.

It is also important to consider that age assurance is often trying to achieve the objective of preventing children and young people accessing content or engaging in online experiences that are age inappropriate. To note:

- Preventing children's access and exposure to harmful content is a primary goal of online safety regulations in many countries, including Australia, with a focus on the role of age assurance.
- Data from eSafety's recent online survey of 3,454 Australian children aged 10 to 17 years showed that many children have, at some stage, encountered content associated with harm online. This includes exposure to content that may fall under the Phase 1 or Phase 2 codes, such as fight videos (47%), sexual images or videos (32%), content depicting or encouraging illegal drug taking (27%), extreme real-life violence (22%), content suggesting how a person can suicide or self-harm (19%) and violent sexual images or videos (12%).
- eSafety recognises that certain sections of the Australian community face higher online risks than others. These harms, as well as measures intended to address these harms, can have differential impacts. This is compounded for disadvantaged, marginalised and underrepresented groups, especially those with intersecting risk factors.
- Children and young people may be at greater risk than adults of experiencing a range of adverse impacts, including to their mental health, as a result of exposure to online content associated with harm and the design of social media services, including features such as the 'like' button and endless scrolling.[4]
- In the case of pornography, eSafety's research with 16-18 year olds indicates that children may be at greater risk of negative impacts when this content is encountered unintentionally. eSafety found that of the young people surveyed who had encountered online pornography, 58% reported they had unintentionally encountered content at least once. One in three (30%) young people who had seen online

[4] American Psychological Association (2023) Health Advisory on Social Media Use in Adolescence, American Psychological Association Health Advisory on Social Media Use in Adolescence; Chhabra J, Pilkington V, Benakovic R, Wilson M, La Sala L, Seidler Z Social Media and Youth Mental Health: Scoping Review of Platform and Policy Recommendations J Med Internet Res 2025;27:e72061; Written Testimony of Mitch Prinstein, PhD, ABPP Chief Science Officer American Psychological Association Protecting Our Children Online Before the U.S. Senate Committee on Judiciary, 14 February 2023, 2023-02-14 - Testimony - Prinstein.pdf.

pornography first encountered content unintentionally before the age of 13. Focus group participants' reflections that unintentional encounters with online pornography can be uncomfortable, distressing and guilt-inducing for young people suggest that such encounters may be harmful to young people. These reflections were consistent with the literature exploring young people's feelings and responses to unintentional and intentional encounters with online pornography.[5]

- The effects of seeing pornography on children and young people are difficult to measure and can be discussed only in terms of correlation, not causation.[6] However, research has found an association between viewing pornography and harmful sexual behaviours in children and young people. A systematic review of literature on the topic found that encountering both violent and non-violent sexually explicit material was associated with problematic sexual behaviour among children and young people.[7] Similarly, research with practitioners and applied researchers found that experts saw using pornography as one of five key risk factors for harmful sexual behaviours among children and young people.[8]

- Pornography depicting strangulation has been associated with viewers engaging in acts of sexual strangulation. While there is little recent, reliable data on the prevalence of sexual strangulation among young people, research has shown that teens in Australia are likely to imitate acts, like strangulation, that they see in pornography.[9] The data relating to adults may be indicative of the practices of teenagers. A recent survey of Australians aged 18-35 found that pornography was the primary way that participants learned about sexual strangulation.[10] The same study found that 57% of participants had been sexually strangled and that 51% had ever strangled a partner, with similar results found among another survey of Australian

[5] British Board of Film Classification (BBFC). 2020. Young People, Pornography and Age- Verification. BBFC. Accessed December 2024. https://www.bbfc.co.uk/about-classification/research Lewis, L., J. Mooney Somers, R. Guy, L. Watchirs-Smith and R.S. Skinner. 2018. 'I See it Everywhere': Young Australians Unintended Exposure to Sexual Content Online.' Sexual Health 15, 335-341. Peterson, A.J., G.K. Silver, H.A. Bell, S.A. Guinosso and K.K. Coyle. 2023. 'Young People's Views on Pornography and their Sexual Development, Attitudes, and Behaviors: A Systematic Review and Synthesis of Qualitative Research.' American Journal of Sexuality Education 18 (2): 171-209.

[6] McKee, A., Litsou, K., Byron, P. and Ingham, R., 2022. What Do We Know About the Effects of Pornography After Fifty Years of Academic Research?. Taylor & Francis.

[7] Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. *Child abuse & neglect*, *143*, 106255.

[8] McKibbin, G., Humphreys, C., Tyler, M, & Spiteri-Staines, A. (2022). Clusters of risk associated with harmful sexual behaviour onset for children and young people: opportunities for early intervention, Journal of Sexual Aggression, September. https://doi.org/10.1080/13552600.2022.2117429

[9] Woodley, G., & Jaunzems, K. (2024). Minimising the Risk: Teen Perspectives on Sexual Choking in Pornography. *M/C Journal*, *27*(4).

[10] Sharman LS, Fitzgerald R, Douglas H. Prevalence of Sexual Strangulation/Choking Among Australian 18-35 Year-Olds. Arch Sex Behav. 2025 Feb;54(2):465-480.

undergraduate students.[11] Both studies found a gendered pattern in this behaviour, with men who have sex with women being more likely to strangle than be strangled, reflecting sexual scripts in pornography.[12] A US based qualitative study found that most women who had been strangled during sex report that it happened without their explicit consent.[13] Pornography has been found to influence young people's perception of sexual strangulation as safe,14 in direct contrast to consensus that this practice is never without risk.[15]

- There are also cohorts within children and young people who are at greater risk of a range of online harms. eSafety research shows that certain cohorts of children, including Aboriginal and Torres Strait Islander children, children with disability and LGBTIQ+ teens, are at greater risk of harm online, including being more likely to encounter content associated with harm online. For example, forthcoming data based on eSafety's 'Keeping Kids Safe Online' survey of 3,454 Australian children aged 10 to 17, shows that lifetime exposure[16] to online content that suggests how a person can self-harm or suicide is heightened certain cohorts. This includes among trans and gender-diverse children[17] (46%), sexually diverse teens[18] (43%), Aboriginal and/or Torres Strait Islander children (31%) and children with disability (27%). Trans and gender-diverse children (37%), Aboriginal and/or Torres Strait Islander children (35%), children with disability (27%) and those from non-English speaking backgrounds (26%) were also more likely to have ever seen extreme real-life violence online (like photos or videos of real people being seriously injured, such as stabbed or killed).

[11] Sharman, L.S., Fitzgerald, R. & Douglas, H. Strangulation During Sex Among Undergraduate Students in Australia: Toward Understanding Participation, Harms, and Education. *Sex Res Soc Policy* 22, 362–375 (2025)
[12] Sharman LS, Fitzgerald R, Douglas H. Prevalence of Sexual Strangulation/Choking Among Australian 18-35 Year-Olds. Arch Sex Behav. 2025 Feb;54(2):465-480.
[13] Herbenick D, Guerra-Reyes L, Patterson C, Rosenstock Gonzalez YR, Wagner C, Zounlome N. "It Was Scary, But Then It Was Kind of Exciting": Young Women's Experiences with Choking During Sex. Arch Sex Behav. 2022 Feb;51(2):1103-1123.
[14] Sharman LS, Fitzgerald R, Douglas H. Prevalence of Sexual Strangulation/Choking Among Australian 18-35 Year-Olds. Arch Sex Behav. 2025 Feb;54(2):465-480.
[15] Woodley, G., & Jaunzems, K. (2024). Minimising the Risk: Teen Perspectives on Sexual Choking in Pornography. *M/C Journal*, *27*(4).
[16] Q: Have you ever seen or heard any of the following things online? You can include things that were said or posted as 'just a joke'. Important: Please don't include things you've seen in TV shows or movies, like on Netflix or Disney+.
[17] The smaller sample size for trans and gender-diverse children should be considered when interpreting these findings (*n*=83).
[18] Sexually diverse' includes participants who identified their sexual orientation as 'gay or lesbian', 'bisexual', 'queer', 'asexual', 'pansexual' or that they are 'still working it out'. Sexuality was asked only of children aged 13–17.

- As noted in the United Nations General Comment No. 25 (2021) on children's rights in relation to the digital environment, the risks and opportunities for children in the digital environment vary with their age and stage of development. Consideration should be given to children's evolving capacities when designing measures to protect children or help them safely access the digital environment.

Industry Codes and Standards

Industry codes and standards under the OSA

The Australian Parliament included in the Online Safety Act a statement of regulatory policy expressly stating its intention that industry bodies develop industry codes in relation to their online activities and that the Commissioner should take reasonable steps to ensure this regulation occurred within 6 months for industry codes, and within 12 months for industry standards.[19]

The Online Safety Act sets out examples of matters that may be dealt with by industry codes and standards, including certain types of harmful online material (Class 1 and Class 2 material)[20] and for eSafety to register and enforce the codes.

Class 1 and Class 2 material are defined under the Online Safety Act by reference to the National Classification Scheme, which is a cooperative arrangement between the Australian, state and territory governments.

Class 1 and Class 2 material constitute a range of harmful content, either because it is illegal, such as child sexual exploitation and abuse, or is inappropriate for children to access, such as online pornography. See Attachment B for further details.

The Parliament, in setting the threshold for the Commissioner's decision to register a code to whether '...the code provides appropriate community safeguards...',[21] intended that codes should sufficiently address both current and, importantly, emerging harms at the time the code is being considered.

Examples of harms emerging since the commencement of the Online Safety Act include harms from artificial intelligence, addressed in the *Internet Search Engine Services Online*

[19] Section 137 of the Act.
[20] Section 138 of the Act. Under the Act, Class 1 and Class 2 material are defined by reference to the classification the material has or would likely be given, under the National Classification Scheme. See Attachment B for further details.
[21] Section 140 of the Act.

Safety Code (Class 1A and Class 1B) and harms from AI companions, addressed in the *Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)*. These harms were not covered in initial drafts and only addressed after the Commissioner raised concerns with industry.

Respective roles and responsibilities

In summary, industry bodies are responsible for:

- Developing the Industry Code that applies to participants in their section of the online industry and giving that code to the Commissioner.
- Inviting members of the public to make submissions on draft codes (for a period of at least 30 days) and have regard to those submissions.

In summary, eSafety's role and responsibilities include:

- Issuing a request for code development: [22] the Commissioner can issue a notice requesting a body representing a section of the online industry develop an industry code for that section of industry.
- Registering a code:[23] the Commissioner may register a code prepared by an industry body if the Commissioner is satisfied that:
    - the code provides appropriate community safeguards for matters of substantial relevance to the community, and other matters are dealt with in appropriate manner
    - the industry body published a draft of the code and invited and considered public and industry submissions about the draft, and
    - the industry body consulted the Commissioner about the development of the code.
- Determining industry standards:[24] if a code does not meet the above statutory requirements, the Commissioner can create industry standards for the relevant online sectors. The eSafety Commissioner must not determine a standard unless satisfied that it is necessary or convenient to provide appropriate community

[22] Section 141 of the Act.
[23] Section 140 of the Act.
[24] Section 145 of the Act.

safeguards or otherwise adequately regulate participants in an online industry section.

- Compliance: eSafety can direct participants covered by the code to comply with the code.[25] It can also receive complaints and investigate potential breaches of the codes or standards.[26] eSafety can also issue a formal warning in response to a contravention.[27] eSafety's measures will be enforceable by civil penalties, infringement notices, enforceable undertakings and injunctions to ensure compliance.[28]

While not a formal requirement of eSafety, in September 2021, eSafety published a position paper to assist the online industry in the development of the industry codes. The paper set out 11 policy positions regarding the substance, design, development and administration of industry codes for Class 1 and Class 2 material, as well as eSafety's preferred outcomes-based model for the codes. At this time, eSafety established that the substance of the codes should address the issues of access, exposure and distribution that are related to Class 1 and Class 2 material.

In eSafety's discussion with industry around how to tackle the codes, it was agreed that industry would adopt a two-phased approach to industry codes. This was to ensure the risks associated with the most harmful material were addressed as a priority and to allow a different approach for content which is inappropriate for children.

On 1 July 2024, eSafety published a position paper setting out principles and suggestions for industry in developing the second phase of the codes (Phase 2 Position Paper). In this paper, eSafety published examples of suggested minimum compliance measures for industry to consider. This includes:

- Applying age assurance across different types of services like social media, search engine services, app distribution platforms, and online pornography providers, in a way that is appropriate and proportionate to risk.
- Creating enforceable requirements for services which disallow types of Class 2 material according to their own terms of service to action that material, including by detecting and removing it.

[25] Subsection 143(1) of the Act.
[26] Section 42 of the Act.
[27] Section 144 of the Act.
[28] Subsection 143(2) and Part 10 of the Act.

- Applying default safety measures like interstitial notices, blurring and filtering of pornographic or violent imagery, on services where age assurance hasn't occurred.
- Making safety tools, options and information available to adult end-users on an opt-in basis.

Key parts

The key parts about the industry codes and standards framework include:

- By legislative design, industry codes are drafted by industry, for industry.[29] Industry is responsible for the content and the measures in the codes.
- The industry-led approach gives industry bodies the opportunity to apply their expertise and technical understanding to develop robust codes. They also lift the bar for the entire online industry – enshrining good practices and meaningful guardrails for apps and services, but also for 'gatekeeper' services such as search engines and app stores.
- The intention is to standardise and uplift industry's safety practices, so the public can be confident they represent what the technology industry itself considers to be proportionate and feasible measures to enhance online safety, especially for children.
- Industry codes are not legislation. eSafety also does not have power to draft the content of industry codes, or to amend a code.[30]
- The Commissioner's decision to register a code is not reviewable under the eSafety internal review scheme or by the Administrative Review Tribunal, as the Online Safety Act only provides that a decision to refuse to register an industry code is a 'reviewable decision'.[31] Any standard created by the eSafety Commissioner is reviewable by Parliament.[32]
- The Online Safety Act sets out public consultation processes, which the industry bodies have complied with.[33] The process of code creation has been publicly promoted by both by eSafety and the responsible industry groups.

[29] Sections 140 & 141 of the Act.
[30] Part 9, Division 7, Subdivision C of the Act.
[31] Subsections 220(17) & (18) of the Act.
[32] Section 145 of the Act and Chapter 3, Part 2 of the *Legislation Act 2003* (Cth).
[33] Subsections 140(e) & (f) of the Act.

In relation to the Phase 2 Codes, industry consulted with the public from October to November 2024. Industry also conducted roundtables to raise questions and incorporate the perspectives of affected industry sections.

Phase 2 Codes

In July 2024, eSafety issued notices asking for two matters to be addressed by industry within the Phase 2 Codes:

- Protect and prevent children in Australia from accessing or being exposed to Class 1C and Class 2 material.
- Provide end-users in Australia with effective information, tools and options to limit access and exposure to Class 1C and Class 2 material.

The Phase 2 Codes deal with material that is legally age-restricted and designated as harmful for children by the Australian Government under the National Classification Scheme.

In summary, material relevant to Phase 2 codes:

- Online pornography and high impact nudity (Class 1C and Class 2A).
- Class 2B material involving high impact violence, drug use and themes such as crime.
- Class 2B material involving other high-impact material (e.g. simulated gambling) and themes (e.g. suicide and serious illness).

As of 9 September 2025, all codes under Phase 2 were registered. This comprises 9 codes, being:

- Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) – Head Terms – 9 September 2025
- Schedule 1 – Hosting Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 2 – Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 3 – Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 4 – Social Media Services (Core Features) Online Safety Code (Class 1C and Class 2 Material)
- Schedule 4A – Social Media Services (Messaging Features) Online Safety Code (Class 1C and Class 2 Material)

- Schedule 5 – Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 6 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 7 – App Distribution Services Online Safety Code (Class 1C and Class 2 Material)
- Schedule 8 – Equipment Online Safety Code (Class 1C and Class 2 Material)

Overarching points about Phase 2 Codes

We note the focus of this inquiry is the Phase 2 Search Engine Code. Before addressing this code specifically, we note some important overarching considerations.

- The new Codes adopt some key good practice measures already being implemented by major platforms. By introducing new obligations that will require more sectors of the online industry to promote children's online safety, they uplift overall safety protections for Australian children.
- The new Codes implement best practice approaches from comparable international jurisdictions. As a result, there can be greater regulatory parity that will enable stronger compliance by industry. This includes:
    - The UK's Online Safety Act 2023, which includes new Codes that require all user-to-user services that allow online pornography to implement 'highly effective age assurance' from 25 July 2025.
    - Ireland's Online Safety Code for Video Sharing Platforms (VSPs) (now in force), which requires the use of effective age assurance measures to ensure that 'adult-only' content cannot be seen by children.
    - The European Union's Digital Services Act, which requires platforms to undertake a range of related measures. This includes risk management frameworks, assessments and mitigations, targeted measures to protect the rights of the child, including age verification and parental control tools, and tools aimed at helping minors signal abuse or obtain support, as appropriate. Guidelines on the protection of minors have just been confirmed, which recommend the use of effective age assurance methods to prevent access to pornography.
    - Singapore's Online Safety Code of Practice for App Distribution Services, which will require designated app stores to implement age assurance to prevent

children downloading age-inappropriate apps (comes into force from 31 March 2026).

- Twenty different states in the United States have passed age assurance laws for access to adult content.

- The Head Terms to the Phase 2 Codes were also drafted by industry. They enshrine principles that will sit alongside the safety measures for every layer of the technology stack. These includes the importance of protecting human rights online, the right to freedom of expression and the requirement for all services to comply with Australian privacy laws. It also includes the rights and best interests of children.
- The Head Terms require providers to take into account the interaction between the Codes and other Australian laws to minimise the collection of personal data.
- In relation to age assurance specifically, the Head Terms list several examples of age assurance measures that could be considered appropriate for the purposes of the Codes. These include, but are not limited to:
  - Matching of photo identification.
  - Facial age estimation.
  - Credit card checks.
  - Digital identity wallets or systems.
  - Attestation by a parent of age or whether an Australian end-user is a child.
  - Use of artificial intelligence technology to estimate age based on relevant data inputs.
- The Heads Terms also specify that in determining appropriate age assurance measures, services must also:
  - Take into account the technical accuracy, robustness, reliability and fairness of the solution for implementing the measure.
  - Consider whether age assurance measures have been designed to comply with privacy laws.
  - Consider whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives.
- Members of industry submitted to eSafety that this formulation of industry-agreed age assurance measures was the right approach to take in the Codes because:

- Services that have the sole or predominant purpose of providing access to age-restricted material like online pornography must implement effective age assurance.
- Key access points to age-restricted material, such as search engines, social media services and app distribution services, must implement effective age assurance if they find themselves to have a high risk-profile.
- Less intrusive measures are included for providers when they opt to adopt effective and enforceable safety measures.

There are specific measures for age assurance in different codes, which are outlined in more detail at Attachment C.

Search Engine Code

In relation to the Search Engine Code, we note the following key points. The specific obligations in the Search Engine Code, as with all other Codes, should be read against the Head Terms.

- By 27 June 2026, search engine services (SES) must implement appropriate age assurance mechanisms for logged-in account holders to ensure that the highest safety settings are applied when a service's systems detect that an account holder is likely to be an Australian child. These obligations do not apply to users who are not logged in. These obligations also don't prevent families from choosing to have a logged in service with shared users, including with identified child profiles (as is currently an option available through Google[34]).
- SES providers must also provide easily accessible and simple-to-use tools to users to:
  - Report thumbnails that contain online pornography and high-impact violence material but are not filtered or blurred on search engines.
  - Enable users to provide feedback about the accessibility of Class 1C and Class 2 material in their search results.
- SES providers will also have enforceable requirements to improve the effectiveness of their safety tools to assess the context of material. This will reduce the risk that SES providers will wrongfully filter or blur material that is permitted under the classification scheme, such as health information.

[34] Google, Manage Search on your child's Google Account - Google For Families Help

- SES providers must also ensure that advertising for online pornography, high-impact violence material and self-harm material is not served to children.
- The Code also provides enhanced protections for users who are not logged in, including:
    - Users who are not logged in will note that sexually explicit or highly violent imagery is blurred by default (but not removed). This will reduce the risk of accidental exposure to this material.
    - Harmful content will be downranked, while authoritative sources will be promoted. For example, if a user enters a search relating to suicide, suicide material will be downranked, while crisis intervention lines will be promoted.
- The age assurance requirements under this code expand on existing practices already routinely applied, whereby if a search engine recognises based on signals that an account holder is a child, safety settings are applied. For example, Google's SafeSearch will already be applied and '*set to Filter automatically when Google's systems indicate that you may be under 18*.'[35]

Social Media Minimum Age

Social Media Minimum Age under the OSA

In December 2024, the Australian Parliament enacted the Online Safety Amendment *(Social Media Minimum Age) Bill 2024* (SMMA Bill), introducing a new Part 4A into the Online Safety Act.

This creates, among other things, an obligation for age-restricted social media platforms to take reasonable steps to prevent Australian children under 16 from having accounts on their platforms (referred to as the 'SMMA obligation' or 'SMMA'). The SMMA obligation takes effect on 10 December 2025.

Respective roles and responsibilities

There are distinct roles for the industry (providers of age-restricted social media service platforms), the Minister for Communications, the Office of the Australian Information

[35] Google, Your SafeSearch Setting.

Commissioner (OAIC) and eSafety in the implementation, oversight and enforcement of the SMMA obligation.

In summary, providers are required to:

- Take reasonable steps to prevent Australian children under 16 (age-restricted users) from having accounts on their platforms.[36]
    - A provider must not collect Government-issued identification material, including using an accredited service within the meaning of the *Digital ID Act 2024,* for the purpose of complying with the SMMA obligation unless a reasonable alternative is provided.[37] They are also restricted from collecting information that is of a kind specified in legislative rules made by the Minister.[38]

In summary, the Minister for Communications is responsible for:

- Making legislative rules specifying services, or classes of services, that are or are not age-restricted social media platforms. In doing so, the Minister must seek and have regard to advice from the eSafety Commissioner.
    - On 19 June 2025, in response to a formal request from the Minister, eSafety provided advice to the Minister on draft legislative rules. On 29 July 2025, the Minister made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 (the Rules), specifying classes of services that are not age-restricted social media platforms.
- Making legislative rules specifying the kinds of information that providers of age-restricted social media platforms must not collect for purposes of complying with the SMMA obligation. In doing so, the Minister must seek and have regard to advice from the eSafety Commissioner and the Information Commissioner. As at September 2025, no such rules have been made or proposed.
- Specifying, by notifiable instrument, a day for the obligations to take effect. The Minister for Communications has specified that the obligation will take effect on 10 December 2025.

[36] Section 63D of the Act.
[37] Section 63DB of the Act.
[38] Section 63DA of the Act.

- Initiating an independent review of the operation of the SMMA. This must be initiated within two years after the day the section 63D obligation takes effect.
    - eSafety is separately conducting an ongoing evaluation of our implementation efforts, supported by an independent advisory panel led by the Social Media Lab at Stanford University that will contribute to the independent review.

In summary, the OAIC is responsible for:

- Functions under the *Privacy Act 1988* that are triggered if there is an interference of an individual.[39]
- Preparing and publishing platform provider notifications if satisfied that an 'age restricted social media platform' has used, disclosed, or failed to destroy certain personal information in a way that is taken to be an interference with privacy.[40]

eSafety is responsible for:

- Formulating and promoting written guidelines for the taking of reasonable steps to prevent age-restricted users having accounts with age-restricted social media platforms. This guidance was published on 16 September 2025.
- Monitoring and enforcing compliance with the SMMA obligation to take reasonable steps.
- Monitoring and enforcing compliance with the requirement to not collect government issued ID or use an accredited service under the *Digital ID Act 2024*, without providing reasonable alternative means, and not collect information specified in any legislative rules.

eSafety does not have a role under the Online Safety Act in formally declaring whether a service meets the criteria to be a certain category of online service under the Act. Similar to other schemes, eSafety does not have a formal role in declaring which services are age-restricted social media platforms for the purposes of the SMMA. However, eSafety's view on whether a service is an age-restricted social media platform will underpin our approach to enforcement. We will provide information about how platforms have self-assessed and our view in the lead up to the commencement of the obligations.

[39] This occurs if a provider uses or discloses personal information of an individual in the circumstances set out in subsection 63F(1) or if a provider does not destroy personal information of an individual in the circumstances set out in subsection 63F(3) of the Act.
[40] This means if the Information Commissioner is satisfied a platform has contravened subsections 63F(1) or 63F(3) of the Act.

Key parts

- eSafety's role under the SMMA is to enforce the laws, as passed by the Australian Parliament. This includes our role to publish guidance on reasonable steps, as well compliance and enforcement.
- The Government assessed that the SMMA Bill is, on balance, compatible with the human rights enshrined in the international instruments to which Australia is a signatory. In particular, the Government found the SMMA Bill supports the best interests of children and the limitations it places on their freedom of expression are reasonable, necessary and proportionate to protect children from harm and uphold their right to health.
- The SMMA obligation puts the onus on social media platforms, not parents or young people, to take reasonable steps to ensure users under 16 years of age do not have accounts on their services. This is about protecting young people, not punishing them.
- eSafety's approach to implementing and enforcing the SMMA obligation will be informed by research, evidence, deep consultation and careful consideration of the best interests of children.
- eSafety undertook consultation with the Australian community, experts and online service providers on the best way to implement social media age restrictions for children under 16. Through multi-stakeholder roundtables and single stakeholder consultations, eSafety engaged with more than 345 people representing over 160 organisations. This included speaking directly with children and young people to inform our approach to implementing the SMMA obligation. The consultation process focused on how eSafety implements its functions under the Act – not on the contents of the legislation itself, which has already been passed by Parliament. eSafety has published information about what we heard from the consultations.
- eSafety has also published an assessment guide for online services to help services determine if they are providers of age-restricted social media platforms. It outlines what services should consider when assessing whether their service includes any of the features and functions listed in these conditions when completing their self-assessment. It sets out a series of steps that will help with the assessment process, including when considering whether a service meets an exclusion under the Rules.
- eSafety has designed an evaluation to monitor the implementation and outcomes of the SMMA. This includes measurement of intended outcomes, and potential unintended consequences. We explore this further below.

- eSafety has publicly spoken about the SMMA operating not as a social media ban, but a social media delay: a delay which gives us vital time to protect young people's health and wellbeing and equip them with the digital literacy and skills they require to engage online safely. This also includes empowering and enabling parents and carers to better engage in their children's online lives.
- Once children turn 16, there will still be risks they face online. Children will also still be able to engage with a range of online services that are not captured by the SMMA. As such, complementing our regulatory work is our prevention and education efforts. This work is critical in keeping all Australians safer on the platforms they are using, encouraging help-seeking behaviour and preparing them for challenges they will face in the future. We explore this further below.
- eSafety continues to take a holistic approach to protecting, supporting and empowering Australian children online. We remain committed to working with teachers, parents, carers and children and young people, including through our Youth Council. This will ensure they are not only well informed about risks, but also well-equipped to thrive online. This is explored further in our eSafety's statement of commitment to children's rights.

Guidelines on reasonable steps

eSafety's function to publish guidelines is intended to assist providers of age-restricted social media platforms in complying with their obligations under the SMMA.

Consistent with stakeholder consultations and the approach of international regulators, eSafety has taken a principles-based approach to this guidance, rather than being prescriptive. eSafety is also mindful of the need to promote all fundamental human rights. This includes the right to privacy, the right to equality and non-discrimination, freedom of expression, access to information and the rights of the child. These underpin all the guiding principles and should be front of mind for providers when implementing measures to meet the obligation.

In the guidance, eSafety identified principles that should inform providers' reasonable steps, including in relation to the use of age assurance. These principles are:

- Reliable, accurate, robust and effective
- Privacy-preserving and data minimising
- Accessible, inclusive and fair
- Transparent

- Proportionate
- Evidence based and responsive to emerging technology and risk
- Respect and protection of fundamental human rights

The guidance provides detailed information to providers about how eSafety suggests that they apply these principles when implementing measures to prevent users under 16 from having an account.

Evaluation

eSafety will be contributing to monitoring and evaluating outcomes of the SMMA. We will examine the extent to which the legislation achieves outcomes aligned with its legislative intent, while also identifying any unintended consequences. In partnership with a lead academic partner and an international and local academic advisory group, we will also monitor the implementation of the legislation and assess its short- and medium-term impacts on children, young people and their parents or caregivers. The evaluation will provide objective, robust evidence to support the independent review of the legislation that must occur within two years of effective commencement of the SMMA, which will be led by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

The primary objectives of the evaluation are to:

- Understand the impacts of the legislation on children and young people and their caregivers, both intended and unintended, over the short- and medium-term.
- Provide objective, robust evidence to inform the independent review of the legislation and adaptations that may be required.
- Contribute to the evidence base on the efficacy of the SMMA.
- Advance knowledge within the Australian context on the broader relationship between social media use and youth mental health.

Complementary measures

eSafety recognises that age restrictions form just one part of a holistic regulatory approach aimed at keeping children and young people safer online. To be effective, technological solutions must be paired with robust education and community engagement strategies.

Through our education and prevention programs, eSafety works across formal and informal education settings to build children's digital literacy, resilience and critical reasoning skills.

We value the importance of embedding online safety into school curricula. To achieve this, we develop age-appropriate education resources and support educators with professional development. We promote greater awareness and cooperation in the 9,653 schools across Australia through the National Online Safety Education Council, which features representatives from all government and non-government education sectors. We support schools accessing best-practice online safety education through the Trusted eSafety Provider program, with participating organisations reaching an audience of over 1.6 million students, educators and parents and carers in 2024-25. We also prioritise outreach to children and young people who face higher risks online, including those from marginalised or underrepresented communities. This ensures tailored and accessible support.

We will continue to engage with children and young people through initiatives like the eSafety Youth Council. This ensures their voices shape the development of resources, campaigns and policy. Our work with parents and carers includes webinars, guides and community events designed to build confidence and foster open conversations about online experiences. These efforts are grounded in child rights principles and informed by ongoing evaluation to ensure relevance and impact. Our goal is to shift online norms by raising awareness and ensuring our regulation is backed by research, education and meaningful community engagement.

We understand concerns that children and young people may feel withdrawn or isolated due to delayed access to certain platforms. This is why our complementary measures focus not only on protection, but also on empowerment, which ensures children and young people are equipped to thrive online, now and in the future.

Conclusion

eSafety is pleased to have had the opportunity to outline Australia's regulatory arrangements for online safety, including eSafety's role and the work we have done to date to acquit our powers and functions. We'll continue to work with all stakeholders as part of a whole of community approach – and especially with children and young people themselves – to promote the safety of children and young people online.

We're happy to provide more information to assist the Committee's inquiry.

Attachment A

Chronology of the development of codes, standards and the social media minimum age restriction

Several milestones relating to eSafety's regulatory remit that were already underway before the inquiry commenced.

We provide a high-level recap of the key milestones below, per this inquiry's focus on industry codes and standards and the SMMA. This includes milestones that were underway before the inquiry commenced and occurring during the inquiry. We have also noted some instances where we made public comments on these milestones.

- **June 2021:** Online Safety Act passed. We published a media release.
- **September 2021:** eSafety released a position paper on the development of industry codes, suggesting a two-phased approach to the development of codes, with Phase 1 focused on Class 1 material such as child sexual exploitation and abuse content, and Phase 2 focused on Class 2 material such as pornography. We published a media release.
- **January 2022:** Online Safety Act commenced. We published a media release.
- **April 2022:** eSafety issued notices formally requesting the development of industry code for Phase 1. We published a media release.
- **June 2023:** Five Phase 1 Codes were registered (Social Media Services (SMS); App Distribution Services; Hosting Services; Internet Carriage Services; Equipment). We published a media release.
- **September 2023:**
    - Phase 1 Code for Search Engine Services was registered.
    - Phase 1 Codes for Relevant Electronic Services (RES) and Designated Internet Services (DIS) were rejected, and Standards development commenced.
    - We issued a media release.
- **December 2023:** Five codes registered in June 2023 took effect. We published a media release. These are due for review by industry after December 2025.
- **March 2024:** Search code registered in September 2023 took effect. We published a media release. This is due for review by industry after March 2026.

- **June 2024:** Industry standards for RES and DIS were registered. We published a media release.
- **July 2024:** eSafety published Notices and Position Paper for the production of Phase 2 Codes. We published a media release.
- **August – November 2024:**
    - Industry associations submitted preliminary Phase 2 Draft Codes for all sections of the online industry. eSafety provided feedback on key issues.
    - The drafting groups conducted public consultation on the Draft Phase 2 Codes during October/November 2024. eSafety promoted the public consultation on our social channels.
    - The drafting groups conducted roundtables with key stakeholders as part of the public consultation process for the Phase 2 Codes.
- **December 2024:** Industry standards for Phase 1 RES and DIS took effect. We published a media release.
- **December 2024:** Industry requested and received an extension of time to return Phase 2 Codes. We published a media release.
- **December 2024:** The Social Media Minimum Age Bill, having passed Parliament in November 2024, received Royal Assent. We published a statement. The obligations are due to commence on 10 December 2025.
- **February-May 2025:** Phase 2 Codes received and eSafety provided feedback. We issued a media release in March. eSafety gave preliminary views on Code registrability in April and sought additional commitments, particularly about chatbots. We published a media release on the final draft industry codes.
- **May 2025:** eSafety called for expressions of interest in being consulted on implementation of the SMMA, including the guidelines that age-restricted social media platforms will have to follow.
- **June 2025:**
    - Enforcement 'grace period' for Phase 1 Industry Standards ends.
    - eSafety Enforcement Taskforce established.
- **June 2025:** eSafety provided advice to the Minister on the draft rules for determining which platforms will not be age restricted.

- **June 2025:** Three Phase 2 Codes Registered (Internet Carriage Services/Hosting Services/Search Engine Services). We published a media release. We also announced this at the National Press Club and published the speech. They will come into effect on 27 December 2025.
- **June - August 2025:** eSafety held stakeholder consultation on the SMMA.
- **July 2025:** Further versions of remainder Codes submitted for assessment. We also published a media release providing information about the Codes process.
- **July 2025:** The Minister made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 and specified 10 December 2025 as the day the SMMA obligation takes effect.
- **September 2025**: Remaining Phase 2 Codes registered. We published a media release.
- **September 2025**: eSafety published summaries of the consultations on the SMMA and a self-assessment tool for online providers to assess whether they are an age-restricted social media platform. We published a press release.
- **September 2025**: eSafety published the SMMA regulatory guidance, including guidelines on the taking of reasonable steps as required under the SMMA obligation, along with eSafety's statement of commitment to children's rights.
- **December 2025:** The SMMA obligations commence.
- **December 2025**: Phase 2 Codes measures start to take effect.

Attachment B

What is 'Class 1 material' and 'Class 2 material'?

Class 1 material is material that is or would likely be refused classification under the National Classification Scheme.[41]

It includes material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified,
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence.

Class 2 material is material that is, or would likely be, classified as either:

- X18+ (or in the case of publications, category 2 restricted) or
- R18+ (or in the case of publications, category 1 restricted) under the National Classification Scheme

Context is important when classifying material. The nature and purpose of the material must be considered, including its literary, artistic or educational merit and whether it serves a medical, legal, social or scientific purpose. This means it is unlikely that sexual health education content, information about sexuality and gender, or health and safety information about drug use and sex will be considered illegal or restricted online content by eSafety.

[41] Classification (Publications, Films and Computer Games) Act 1995.

In our Codes Position Papers, eSafety suggested that industry could consider sub-categories of these classes.

Phase	Class subcategory	Material	National Classification Scheme
Phase 1	Class 1A	• CSEM – Child sexual exploitation material. Material that promotes or provides instruction of paedophile activity. • Pro-terror content – Material that advocates the doing of a terrorist act (including terrorist manifestos). • Extreme crime and violence – Material that describes, depicts, expresses or otherwise deals with matters of extreme crime, cruelty or violence (including sexual violence) without justification. For example, murder, suicide, torture and rape. Material that promotes, incites or instructs in matters of extreme crime or violence.	• Class 1 • Refused Classification
Phase 1	Class 1B	• Crime and violence – Material that describes, depicts, expresses or otherwise deals with matters of crime, cruelty or violence without justification. Material that promotes, incites or instructs in matters of crime or violence. • Drug-related content – Material that describes, depicts, expresses or otherwise deals with matters of drug misuse or addiction without justification. Material which includes detailed instruction or promotion of proscribed drug use	• Class 1 • Refused Classification
Phase 2	Class 1C	• Online pornography – material that describes or depicts specific fetish practices or fantasies.	• Class 1 • Refused Classification
Phase 2	Class 2A	• Online pornography – other sexually explicit material that depicts actual (not simulated) sex between consenting adults.	• Class 2 • X18+

Phase 2	Class 2B	• Online pornography – material which includes realistically simulated sexual activity between adults. Material which includes high-impact nudity. • Other high-impact material which includes high impact sex, nudity, violence, drug use, language and themes. 'Themes' includes social Issues such as crime, suicide, drug and alcohol dependency, death, serious illness, family breakdown and racism. • Simulated gambling in computer games	• Class 2 • R 18+

Phase 1 focuses on high-end Class 1 material (1A and 1B) including child sexual exploitation material and pro-terror content. The primary goal here is to prevent or restrict access to material that poses harm to people of all ages.

Phase 2 covers online pornography (Class 1C and Class 2 material) and other class 2 content. This phase aims to prevent children from accessing age-inappropriate material and offers users effective tools to manage exposure to Class 2 content they do not want to see.

Attachment C

Summary of age assurance measures across Phase 2 Codes

Code	Age Assurance measures
Search Engine Services Code	27 June 2026, search engine services must implement appropriate age assurance measures for **logged-in account** holders. This means logged out users, or users without an account will not have to undergo age assurance when using a search engine.
Designated Internet Services Code	Websites that have the highest risk of enabling children to access or be exposed to pornography and self-harm material must implement appropriate age assurance measures. This includes online pornography sites. Generative AI services that have the highest risk of enabling children to generate online pornography, self-harm material and high-impact violence material must implement appropriate age assurance and access control measures to stop them accessing these features.
Relevant Electronic Services Code	Relevant electronic services with the sole or predominant purpose of permitting end-users to share online pornography or self-harm material must implement appropriate age assurance measures before providing access to the service. If services have AI companion chatbot features, they must follow measures based on the risk of children generating online pornography, self-harm material and high-impact violence material. This includes appropriate age assurance measures for the services with the highest risk.

	Providers of video games rated R18+ by the National Classification Board must also implement appropriate age assurance measures before providing access to the game
Social Media Services (Core Features) Code	Social media services that allow online pornography or self-harm material on their service must implement appropriate age assurance measures before allowing access to this material. If services have AI companion chatbot features, they must follow measures based on the risk of children generating online pornography, self-harm material and high-impact violence material. This includes appropriate age assurance measures for the services with the highest risk.
App Distribution Services	9 September 2026 (six months after the Code comes into effect), app distribution services must implement appropriate age assurance measures before permitting end-users to download or purchase apps rated as 18+.
Internet Carriage Services Code	Nil
Hosting Services Code	Nil
Equipment Providers Code	Nil