Draft Children's Online Privacy Code: eSafety Submission

July 2026

Overview

The eSafety Commissioner (eSafety) welcomes the opportunity to provide a submission to the Office of the Australian Information Commissioner's (OAIC) consultation on the draft Children's Online Privacy Code (draft Code) and Explanatory Memorandum (draft EM).

The Children's Online Privacy Code is an important milestone in Australia's privacy reform and the protection of children online.

Online safety and privacy are mutually reinforcing and closely intersecting concepts. These close connections are reflected in the statutory requirement for the OAIC to consult eSafety in the development of the Code, the close working relationship between the two regulators and our shared priority to better protect Australian children online.

eSafety supports a holistic and coordinated response to ensuring the objectives, compliance and enforcement of the Children's Online Privacy Code and eSafety's regulatory schemes work in a complementary manner. As such, our submission will focus on key intersections between the draft Code and existing and proposed regulatory measures under the *Online Safety Act 2021* (Cth) (Online Safety Act) and our commitment to regulatory coherence, coordination and cooperation.

eSafety's role and regulatory position

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.

eSafety takes a harm-minimisation and risks-based approach. This balances holding industry to account, driving safety uplift through systemic reform and Safety by Design, ensuring the onus of safety is not on the user and upholding human rights, including children's rights.

There is a legislative requirement for the eSafety Commissioner to have regard to the Convention on the Rights of the Child in the performance of her functions relating to children.[1] Consistent with this, eSafety supports a regulatory approach that protects and upholds the rights of children and requires online services to prioritise the best interests and evolving capacities of children.

In September 2025, eSafety published a **statement of commitment**, which provides further detail of this approach and outlines eSafety's actions to support children's rights.

[1] Section 24 of the Online Safety Act 2021 (Cth)

Intersections between the Code and Online Safety Act

eSafety is responsible for several regulatory schemes under the Online Safety Act.

Noting the responsibility of regulators is to implement legislation as passed by Parliament, we have focused on how we can work with the OAIC to collaboratively and cooperatively implement our respective schemes. Our intention is to share regulatory insights, support understanding and compliance with these intersecting obligations, and promote overall coherence to the extent possible.

Given the draft Code applies to relevant electronic services (RES), social media services (SMS), or designated internet services (DIS)[2] as defined in the Online Safety Act, we have focused on schemes where those entities may be subject to both the Children's Online Privacy Code and eSafety's regulatory schemes and there are likely to be significant intersections.

This includes the Online Safety Codes and Standards (comprising of the Unlawful Material Codes and Standards and the Age-Restricted Material Codes), and the Social Media Minimum Age (SMMA) scheme.

Further information about the scope and operation of these schemes is included at **Attachment A.**

Application and scope

The draft Code is binding on APP entities that, among other factors, are providers of a RES, SMS or DIS. These terms are defined with reference to their definition under the Online Safety Act. This means many of the same entities will be governed by both the draft Code and other online safety requirements, including the existing Online Safety Codes and Standards, and SMMA obligation.

Due to the converging nature of online services, it can be challenging to categorise them under legislative definitions. For example, there is significant overlap between services whose primary purpose is to enable online social interaction under the definition of SMS, and those that may be classified as an instant messaging or chat service under the definition of RES. While DIS are defined to the exclusion of SMS and RES, services which may have started out in this category may subsequently introduce features which could make them more aligned with SMS and RES definitions. Under the Online Safety Act, obligations can vary for different services, but are broadly risk- and outcomes-based, and technology neutral. As the draft Code proposes these services will have the same obligations, this will

[2] Defined under the draft Code with reference to the definitions in Part 1 of the Online Safety Act 2021 (Cth).

increase certainty and consistency and avoid potential confusion over scope or varying obligations.

Obligations under eSafety's schemes will intersect with requirements in the draft Code. For example, the use of age assurance across different services.

While complementary intersections may also incentivise compliance and encourage both safety and privacy uplift for services, overlapping requirements may cause confusion for industry and the public.

It will be important for eSafety and the OAIC to work closely on key messaging and guidance to support understanding of these obligations.

In doing this, eSafety will build upon the regulatory guidance it has published for its schemes and insights from its engagement with industry. It will also build upon learnings from the SMMA. This includes the co-regulatory approach it followed with the OAIC and implementation work regarding engagements with regulated entities.

Children's safety

As outlined above, eSafety supports a regulatory approach that protects and upholds the rights of children and operates in their best interests.

eSafety notes that certain safety protections that enable and promote the best interests of the child, such as requiring services to have default safety provisions to keep children safe, necessarily require the handling of some personal information to verify the user is a child.

eSafety therefore encourages the OAIC to consider how the draft Code's requirements may affect existing safety measures that services have in place, especially for children, to avoid unintended consequences.

For example, regarding the requirement under section 9 that entities may collect personal information about a child by default only if strictly necessary, we encourage the OAIC to clarify in the Code that 'strictly necessary' includes for the purpose of applying safety tools, such as those which seek to prevent and address child sexual exploitation and abuse, grooming and sexual extortion, or prevent children's access to age-inappropriate material, where those tools rely on personal information.

Some safety tools, such as grooming detection technology, combine textual analysis with indicators such as users' ages, locations and usage patterns, to detect likely grooming by an adult with a child. This necessarily requires the processing of personal information.

Services also use behavioural signals to identify other risks to children. For example, if an adult in another jurisdiction adds lots of Australian children as 'friends' in a short period of time, those accounts can be blocked from being recommended to child accounts, or the

platforms can provide notifications to the accounts they interact with, providing safety advice. Where confidence is high, a platform may investigate further.

If section 9 has the effect of limiting services' ability to collect and process the personal information that enables these tools, it may lessen protections for children. We suggest that when determining whether collection is strictly necessary, providers should need to take account of the best interests of the child.

eSafety encourages platforms to ensure their safety efforts are constantly improving, in response to changes in their platforms' features, functions, and end-user practices, particularly where these or other changes may introduce new risks for children. In the context of the SMMA obligation, eSafety considers it reasonable that platforms should be monitoring, uplifting and seeking to improve the reliability, robustness and effectiveness of their measures over time. We also encourage the OAIC to provide clarity and guidance to industry on the application of the draft Code, and in particular section 9, to these circumstances, including if or when the child's (or a person with parental responsibility) consent is required, and how the best interests of the child can be applied.

We also note safety is not expressly drawn out as a matter to be considered across several key provisions in the draft Code. We encourage the OAIC to consider children's online safety risk factors as being relevant risk factors for the draft Code, as well as determining what information is strictly necessary and in the best interests of the child. This would be consistent with how eSafety regularly considers privacy risks in both the creation and implementation of online safety regulations.[3] It would also further promote understanding that privacy and safety are mutually reinforcing and supporting objectives.

Age assurance obligations

Providers of certain online services are required to implement age assurance across several regulatory schemes under the Online Safety Act, including the SMMA scheme, the Age-Restricted Material codes, the Basic Online Safety Expectations (Expectations) and the Restricted Access System Declaration.

In certain cases, the draft Code requires entities to take steps that are reasonable in the circumstances to ascertain the age of an end-user before collecting personal information. The Explanatory Memorandum establishes that 'reasonable in the circumstances' depends on the risk of harm that may arise from any collection, use or disclosure of the end-user's personal information. While this aligns with eSafety's risk-based approach to the use of age assurance, the relevant risk factors are different. Under the SMMA and the Age-Restricted

[3] For one example, see clause 5.1(c)(iii) of the Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms; and associated Regulatory Guidance)

Material Codes, services are encouraged to consider the risk to children, including access to certain age-inappropriate content, among other factors including impacts on privacy, when determining what age assurance is appropriate.

eSafety notes the importance of enabling consistency in how age assurance measures are implemented across different regulatory frameworks. In practice, many regulated entities will be subject to multiple obligations requiring them to assess or infer user age, including under the draft Code, the Age-Restricted Material Codes, and the SMMA. Across these three frameworks, there are different relevant age thresholds, of 15, 16 and 18. The OAIC may consider guidance enabling industry to adopt higher age thresholds for the purposes of the consent provisions, such as 16, to allow for a more consistent and streamlined regulatory approach by reducing the number of age thresholds they must apply.

In addition to establishing the applicable age thresholds, services will also need to consider what method(s) of age assurance to use and where or when within the user journey to apply the(se) method(s). Under the SMMA Regulatory Guidance, eSafety takes a flexible, principles-based approach and does not prescribe technologies nor when to use them. eSafety's Guidance is clear that self-declaration on its own is not sufficient to meet the SMMA obligation, but in some circumstances, it may be reasonable to have self-declaration at sign-up if it is backed up by measures such as robust age inference tools, effective underage user reporting mechanisms, additional forms of age estimation or verification, and measures to prevent removed users from re-creating accounts.

Under the draft Code, it is likely some services will be required to use stronger forms of age assurance than self-declaration at the point when a user signs up, to prevent the service from collecting data about children for purposes other than confirming their age. To the extent this applies to age-restricted social media platforms, OAIC and eSafety will need to continue working together to support services and users in understanding changes that may need to occur to existing processes to meet the requirements of both frameworks.

It is our understanding that nothing in the draft Code would prevent services from applying the waterfall, or successive validation, approach that eSafety recommends in our SMMA Regulatory Guidance. This is important, as a waterfall approach requires providers to have processes to detect users that may have circumvented an initial age check, for example, by deploying tactics to look older or using someone else's ID.

A waterfall approach also acknowledges that age assurance is an ongoing process that services will need to continue working on over time to re-establish or build cumulative confidence in the service's understanding of the age of a user. An age check upon sign-up is not sufficient to determine a user's age in perpetuity, given the risks of circumvention either at the time, or afterwards (for example, if an age-verified account is sold or gifted to

someone younger). Instead, services should actively monitor for signals that a user may be underage and require them to undergo another age check where appropriate.

Facilitating the appropriate re-use of age assurance outcomes or signals across these frameworks is one example that could reduce duplication in the collection of information, support more consistent user experiences, and improve overall safety and privacy outcomes.

Commencement of the Code

We note that the OAIC is seeking views on the commencement arrangements for the Code, which must be registered by 10 December 2026.

While this is ultimately a decision for the OAIC, we note some operational factors that the OAIC may want to consider in determining when the Code takes effect, including the possibility of varying transitional periods.

eSafety's experience with the implementation of the SMMA and Online Safety Codes and Standards indicates that sufficient lead time, transitional arrangements where appropriate[4] and early engagement with regulated entities are important to support effective and consistent compliance.

eSafety also notes there is other reform relating to digital platforms occurring across the relevant period. Within eSafety's remit, this includes:

- The Government has committed to legislate a duty of care as an immediate priority, among other reforms addressed in the Independent Review of the Online Safety Act. In its response to the review, the Government has stated that work is underway to introduce a Bill into Parliament on the duty of care, consistent with the Government's legislative priorities. This is likely to include a transition period after Royal Assent.
- Industry associations are currently conducting a review of the Unlawful Material Codes, as required by the Head Terms.
- The Minister must cause to be conducted a review of the SMMA obligations within two years of it taking effect, being December 2027.

Given the parallel processes underway over the same timeframe, we welcome the opportunity to continue engaging with the OAIC.

[4] For example, the ARM Codes took a staggered approach to commencement, with provisions relating to age assurance taking effect later than other provisions.

Continuing to work together

eSafety is committed to continuing to work with the OAIC to share regulatory insights and approaches in support of a coherent regulatory environment, including in relation to the Code.

We therefore encourage information sharing on potential regulatory and compliance issues that can assist and inform enforcement of our respective schemes.

The constantly evolving regulatory environment, including the development and implementation of the duty of care under the Online Safety Act, also underscores the need for eSafety and OAIC to continue engaging closely on shared priorities and cohesive regulatory efforts.

eSafety is pleased that this may now be formally facilitated under the **Memorandum of Understanding** between the agencies that was entered into in early 2026. This formalises an existing strong collaborative relationship between the two agencies.

Additionally, as in practice there are close intersections between people's experience of safety and privacy online, eSafety can continue to share insights from our prevention, education and engagement work with young people, parents, carers and educators, among others.

We also welcome the opportunity to facilitate a connection for the OAIC to engage with the eSafety **Youth Council** to further embed the lived experiences and perspectives of children and young people into online safety and privacy approaches.

Conclusion

eSafety is pleased to have the opportunity to contribute to the development of this important pillar of protection for children online.

eSafety looks forward to continuing to work closely with the OAIC in the implementation of our regulatory schemes, and in our efforts to create safer and privacy-preserving online experiences for Australian children.

We are happy to provide any further information that would be of assistance.

Attachment A

Online Safety Codes and Standards

The OSA provides eSafety with legislative powers to register and enforce Online Safety Codes and Standards relating to unlawful and age-restricted material online (often referred to as 'illegal and restricted online content').[5] The aim of the Codes and Standards is to address systemic risks and focus on proactive and systemic change.

The Codes and Standards apply to eight sections of the online industry[6]: social media services, relevant electronic services, designated internet services, search engine services, app distribution services, hosting services and internet carriage services. All Codes and Standards are available at the **Register of Online Safety Codes and Standards.**

eSafety notes that the draft Children's Online Privacy Code has adopted the definitions of social media services, relevant electronic services, and designated internet services from the Online Safety Act.

Age-restricted social media platforms, as defined in Section 63C of the Act, also have obligations under the Codes and Standards. This ensures that there are protections for all users, including for users with age-restricted social media platforms such as 16- to 17-year old users.

Throughout the online safety codes and standards and like in the draft Code, qualifying terms such as 'reasonable' and 'appropriate' are used to ensure that obligations are proportionate to the size of a service and the risk of harm. For example, section 11 in both the Unlawful Material Relevant Electronic Services Standard[7] (RES Standard) and Designated Internet Services Standard lists factors which industry must take into account when complying with certain measures.

While the Unlawful Material Codes and Standards are focused on reducing risks associated with unlawful material, the RES Standard contains requirements which address risks of adults contacting young Australian children (defined as under 16).[8] Service providers may implement age assurance to comply with these requirements.

---

[5] This is called Class 1 and Class 2 material in the OSA. Class 1 and class 2 material ranges from the most seriously harmful types of content, such as material showing the sexual abuse of children or promoting acts of terrorism, through to material which is inappropriate for children, such as online pornography.
[6] Section 135 of the Online Safety Act 2021
[7] *Online Safety (Relevant Electronic Services – Class 1A and Class 1B Material) Industry Standard 2024.*
[8] See section 18(4) of the RES Standard.

Age-Restricted Material Codes

Under the Age-Restricted Material Codes, providers of certain high-risk services will be required to implement appropriate age assurance measures and then take steps to prevent children (under 18) from accessing or being exposed to class 1C and class 2 material on their service.

Age assurance requirements in the codes reflect the risk that a provider's service could be used to expose children to class 1C and class 2 material on that service. These requirements are technology neutral, allowing service providers to choose how best to meet the required outcomes within their existing framework of operations.

Age assurance measures must be 'appropriate'. The Head Terms to the Age-Restricted Material Codes provides that self-declaration and contractual restrictions would not be considered 'appropriate', and that service providers should take into account the technical accuracy, robustness, reliability and fairness of their measures. Service providers must also consider whether age assurance measures comply with Privacy Laws and whether the impact on user privacy of any such measures for a service is proportionate to the online safety objectives. Detailed information about age assurance requirements under the Age-Restricted Material Codes is included in eSafety's **Online Safety Codes and Standards Regulatory Guidance**.

Social Media Minimum Age

Section 63D of the *Online Safety Act 2021* (Cth) requires providers of 'age-restricted social media platforms' to take reasonable steps to prevent Australian children under 16 years of age from having accounts on their platforms from 10 December 2025 (the Social Media Minimum Age obligation, or SMMA). Broadly speaking, reasonable steps consist of systems, technologies, people, processes, policies and communications that support compliance with the SMMA obligation – including the use of age assurance.

eSafety published **Regulatory Guidance for the Social Media Minimum Age** in September 2025. The Regulatory Guidance sets out guiding principles to inform the taking of reasonable steps; steps should be:

- Reliable, accurate robust and effective
- Privacy-preserving and data-minimising
- Accessible inclusive and fair
- Transparency
- Proportionate
- Evidence based and responsive to emerging technologies and risk

eSafety consulted with the OAIC on the development of the Regulatory Guidance.

eSafety and the OAIC share regulatory responsibilities under the SMMA. As ss 63F(1) and (3) of the *Online Safety Act 2021* (Cth) are taken to be an interference with the privacy of an individual if breached, it is the responsibility of the Information Commissioner to enforce them.