submission number and name	issue description	Response
1. Qoria	Our biggest concern with the proposed Codes is that Schedule 7 (Equipment Online Safety Code) fails to tackle issues with parental controls inc requirements from schools that they are not used on school devices. We urge that the codes be reviewed to require that Operating System Providers provide safety features including user identification, filtering and reporting and provide interoperable access to 3rd party developers.	This concern is noted. Under the OSA it is beyond scope of Codes to make commitments to third parties other than eSafety
2 Sam Nicholas	The reform's approach to prohibiting content may unintentionally encourage piracy. Simply put, if you want to reduce piracy, make content accessible, both in cost and ease of access. If you want to increase piracy, make the content impossible to obtain legally. By limiting access to the content that minors want to access, the proposed reforms could instead foster an environment of increased, self-justified piracy, and open the doors to accessing totally unmoderated content. This represents lost revenue for the games industry, but it also exposes minors to completely unmoderated channels, as well as potential malware and spyware on their devices. Concerned about scope of definitions of simulated gambling for games	eSafety has made clear in the position paper that at a minimum it requires access to Class 1C and certain types of Class 2 materials to be restricted to under 18 year old users in conformity with the approach offline under the National Classification Scheme. Further refinements have been made in the Codes to the definitions of games in scope.
3 Brian Walker	Expletive	Nil
4 Dalgarno Institute	The combination of social media addiction and substance promotion creates compounded risks for young users.Platforms exploit psychological vulnerabilities through: ◊ Variable reward schedules ◊ Social validation loops ◊ Fear of missing out (FOMO) ◊ Continuous scroll mechanisms. Recommendations: A. Mandatory government ID verification for account creation B. Regular age verification checks C. Age-appropriate content filters D. Financial penalties for verification failures D Mandatory AI-powered content detection E. Required takedown timeframes F. Algorithm transparency requirements G Regular content audits H Cross-platform coordination requirements. I Mandatory warning systems J. Required intervention points K Access to support service L Usage tracking and alerts M Mandatory cool-down periods N Mandatory disclosure of paid promotion by influencers O. Restrictions on substance-related content from high-influence accounts P. Age-gating for accounts promoting adult-oriented lifestyles Q. Requirements for health warnings on lifestyle content featuring substances R. Mandatory usage limits and breaks S. Removal of infinite scroll features T Restrictions on engagement metrics for young user. U. Require digital wellness tools V. Transparent reporting of addictive design features. Other recommendations relate to penalties and enforcement.	We acknowledge the concern of the Institute about the risks of substance promotion online. The issues associated with promotion of illegal drug-related materials has largely been tackled in the Phase 1 Codes and Standards. It is beyond the scope of these Codes to deal with penalties but we draw you attention to recent amendments to the OSA in November 2024 that mandated age-restrictions for specific categories of social media services and increased penalties for Code breaches to a maximum of 49.5 million AUD.

submission number and name	issue description	Response
5 Australian Youth Affairs Coalition	A. AYAC recommends that data should only be collected through age assurance when it is strictly necessary. B. AYAC recommends that platforms must be clear about what data is collected, why it is being collected, how long it is stored for and its uses. C. AYAC recommends that platforms do more to ensure that there are young person friendly explainers of terms and conditions when age assurance is sought. D. AYAC recommends that the Online Safety Team review the concerns around enforceability and utility raised by policy experts and explain to young people in an accessible way how these are being mitigated to enhance their confidence in the codes. E. AYAC recommends that more can be done to empower young people through ongoing collaboration and codesign where their perspectives are engaged with meaningfully and incorporated into the development of the codes. F. AYAC recommends that industry and policymakers work closely with the youth sector to develop repertoires of engagement that facilitate the active participation of young people. G.AYAC recommends the appointment of an independent auditor charged reporting on the quality of youth engagement and suggesting areas of improvement.	The Head Terms requires companies to consider users privacy generally in implementing age assurance under the Codes Additionally, we note requirements around privacy and data minimisation are dealt with by the Privacy Act AAP 13. The Codes include requirements to ensure that terms and conditions are clear and accessible. The remaining issues are not in scope but relate to the operation of the OSA regime generally. In this regard we draw your attention to the ongoing rolling reform of Australian privacy law including the new Privacy and Other Legislation Amendment Act 2024 (which, amongst other things, introduced a statutory tort for serious invasions of privacy and , provisions regarding a Children's Online Privacy Code and obligations regarding use of personal information for automated decision making) may also impact the implementation and use of age assurance measures by organisations and how information may be used in connection with that. In particular, there is a likely intersection between the Phase 2 Codes and the forthcoming Children's Online Privacy Code to be developed by the OAIC.
6 Khan Sheenan	*issue description*	See response to updated submission below.

submission number and name	issue description	Response
7 Khan Sheenan updated	A.Strengthen Age Verification for Restricted Content The Phase 2 codes should mandate advanced age assurance technologies to prevent underage access to high-impact materials, including pornography and other harmful content. Current measures, such as landing pages requiring only a single click, are inadequate. Implementing robust age verification methods, such as ID verification or parental consent mechanisms, would significantly reduce the exposure of young people to content that negatively influences their mental health and behaviour. Concerns about AI chatbots also raised. B. Increased Accountability for Harmful Content Online platforms must be held accountable for hosting content that promotes or normalizes illegal, harmful, or exploitative behaviours. This responsibility should include a clear mandate for social media and pornographic sites to actively monitor and remove material that depicts coercive acts, even when portrayed as consensual. Platforms should also be required to track and report problematic content patterns, with penalties for non-compliance. This increased accountability would prevent harmful content from shaping young people's understanding of relationships and boundaries. C Improved Risk Assessment and Mitigation Strategies A comprehensive approach to risk assessment must account for the evolving influence of new technologies, including AI and generative content platforms. Emerging technologies can unintentionally expose children to inappropriate material or facilitate risky interactions. Regular audits, proactive monitoring, and regulatory oversight can help identify and address potential risks posed by technological advancements before they become widespread issues. This would include monitoring AI platforms to ensure they do not foster harmful ideologies or self-destructive behaviours. D Educational Initiatives on Digital Literacy and Safety Educating young people on digital literacy and online safety is crucial in helping them navigate today's digital landscape. Schools should implement programs that teach safe online interactions, critical media evaluation, and healthy relationship norms. By embedding digital literacy in educational settings, we can equip children and teenagers with the skills to discern harmful content, recognize red flags in online interactions, and seek help when needed. E More Accessible Reporting and Support Services Online platforms must improve their reporting tools to provide young users with safe, straightforward avenues to report abuse, coercive behaviour, or exposure to harmful content. These tools should be easily accessible, highly visible, and designed to encourage young users to seek help	This feedback has been considered in drafting measures under the Codes. A.The Codes do not mandate a specific method of age assurance but list specific requirements that age assurance methods must meet. The Head Terms exclude single click mechanisms as a means of age verification. B. As set out in eSafety's Position paper the Phase 2 Codes relate to lawful pornographic materials but they do not prohibit specific types of pornography; that is beyond the scope of this project. The Codes are subject to the penalty regime under the OSA. If registered the penalties for breach include fines up to 49.5 million AUD. C. The approach to risk assessment makes clear that technological changes to services including AI -related changes must be taken into account and where significant, notified to the eSafety Commissioner. D. This is out of scope of this process. E. Relevant Codes include requirements about professional resources.

submission number and name	issue description	Response
8 eSafety Youth Council Member	1.The user base of many social media and online platforms are predominantly young people, many of which are under the age of 18. While the age assurance trial continues in Australia, I find it unwise to draft codes related to age assurance before there are more concrete regulations and directions around age assurance. 2. Extending the use of digital 'ecosystems' as described by eSafety and within the draft codes, currently seems the most reasonable direction as digital 'ecosystems' are already a growing tool. Similarly, connected accounts between younger users and their guardians (parents or carers), such as the Messenger Kids function on Facebook can also provide a reliable supervision connection between carers and young children so that the focus is on carer-discretion rather than in-app or in-platform based restrictions and filtering (even though they are independently successful to an extent). 3. Above all, I believe that the most comprehensive safety measures in the online world can be provided by carers and educators close to young people. Social media and digital tools are an inescapable aspect of daily life, and restricting access to social media or digital tools as a whole until the age of 18 reduces connection, cultural/educational exposure, and skill-building opportunities for young people.	The Government has addressed the question of age verification for access to social media in amendments made to the Online Safety Act in November 2024 which restrict under 16 year old users from having an account on certain platforms. Your thoughtful views on the important role of parents and carers and how to promote online safety are noted and much appreciated.
9 Alannah and Madeline Foundation	To uphold children's rights, we maintain the draft codes need the following: • A stronger commitment that age assurance measures will be rights-respecting, user-friendly and proportionate to risk, with a data minimisation approach which protects children's privacy. • Clearer alignment with the understanding of pornography articulated by e Safety, which recognises the impacts of new technologies like generative AI. • Appropriately robust default safety settings for all digital products and services likely to be used by children, not just those which formally permit high-impact material. • More in-depth approaches to risk assessment in relation to children's rights. • Appropriate safety tools and settings offered to families with children under 18, not just under 13. • A more meaningful commitment to community engagement, especially with young people.	A. age assurance requirements in the Head Terms have been updated. However, we are unable to be as prescriptive as suggested regarding the requirements for age assurance pending the outcome of the age assurance trial. B. the definition of online pornography has been updated to better align with eSafety's understanding within the constraints of the Classification Scheme. This includes AI generated materials. B. The Head Terms have been updated by an additional note to clarify the meaning of the.rights of the child as a relevant consideration in judging the appropriateness of measures C. The safety settings e.g for equipment updated in response to this feedback. However, we do not think it is appropriate for families to have same degree of control over internet use for all children under 18 which may run counter to the rights and best interests of the child.
10 QLD Family and Child Commission	Urges that we involve young people in consultation and suggest we refer to eSafety research on Young People and Pornography.	The time allowed for development of these Codes did not allow for direct engagement with young people which we agree would be desirable. We have had regard to eSafety's research and publicly expressed views of the Youth Advisory Council in drafting these Codes. The definitions of online pornography have been updated taking into account this feedback within the constraints of the National Classification Scheme.

submission number and name	issue description	Response
11 Australian Child Rights Taskforce	We support the extension of the codes to address violent content as well as pornography, self-harm material, and simulated gambling. We support a broad definition of online pornography such as that proposed by the eSafety Commission in its Position Paper which includes 'realistically simulated, generated and animated sexual content; high-impact text-based sexual content, including interactive services such as chatbots and AI models providing pornographic content; and high-impact nudity.' We support the inclusion of risk assessment mechanisms and requirements. These mechanisms must include risk of harm to users and not be limited to the functionality of devices. We do not support the limitation of a requirement for evidence of the use by a significant number of children as users to trigger assessment and preventive action. We support the use of default settings as preliminary (but not determinative) mechanisms to reduce the risk of harm. We remain unconvinced of the value and efficacy of age assurance mechanisms as blanket and arbitrary measures unless there is the ability to address the individual circumstances of children and young people. We support the view that the Codes should address and acknowledge issues of privacy and prohibit invasive or unreasonable data practices. We encourage attention to international models of best practice, and coordination with effective implementation across national boundaries. We support a systemic approach to regulation that not only captures deliberate actions and actors but also accidental or incidental harms and risks that may arise in a rapidly developing technological space. We are unclear about children and young people's engagement in the drafting of this Code, and would support their engagement as a way to both improve the Codes and realise children's rights.	Noted. The definitions of online pornography have been updated with this feedback in mind within the constraints of the National Classification Scheme. The short time frame allowed has limited ability to engage with young people directly but we have taken into account public views of the eSafety Youth Advisory Council. We have taken into account best practice models (which are limited) such as the UK Online Safety Act Codes and the UK regulator's guidance on age assurance.

submission number and name	issue description	Response
12 Yoti	The definition of age assurance as currently laid out fails to account for the fact that age assurance is not always used to 'verify the exact age or age range of a given user'. Age assurance can also be used to assess whether a user is below or above an age threshold, such as a minimum, legal age required to access content or purchase age-restricted goods and services. The Head terms should go further and set numerical accuracy objectives and thresholds. In responses to other similar consultations, we have suggested that solutions should be audited, and meet high reliability and attack detection rates. We think industry participants should go beyond simply seeking 'to limit' circumvention 'where reasonably possible'. The eSafety Commissioner should conduct annual reviews of age assurance solutions deployed on the market. This annual assessment should also include the effectiveness of those solutions, and as part of this how easily they can be circumvented. This should be a consideration in the choice of an age assurance method. Credit card checks should not be a method for inclusion reasons. Codes should be enforceable three months after consultation. Code reviews should be by the regulator wit public consultation.	There is currently no international standard which the industry can use to set benchmarks for age assurance, although these are under dvelopment and may be concluded in 2 -3 years.. In the time available for this Code it is not possible to draft performance crietria for age assurance, which may be over-taken by international standards when these are developed. We consider that these issues are better adressed following the outcome of the age assurance trial.
13 Australian and New Zealand Screen Association	Supports approach of DIS Code to Classified DIS. ANZSA's view is that, in line with the approach in the draft Codes, these additional protections would not be appropriate for content which may include these "high-impact" themes, but which have already been classified as R18+.	Noted.
14 Jenna Love	The language in the Codes as they currently read comes across as puritanical and anti-sex. That may not be the intention of onlinesafety.org.au, but it is definitely the outcome. The pendulum needs to swing back towards the centre and take a more measured, less emotive approach to adult sexual expression online. Removing the terms 'high impact' and 'seriously harmful' is important. The more clinical '1C' and '2A' (as per the Act) are preferable. Codes should be cleaer to extent apply to online sex work.	We have updated definitions relating to pornographic materials to take into consideration this concern.

submission number and name	issue description	Response
15 Craig Thomler	The Code regime under OSA is not nuanced. 1. Revised Penalty Structure by introducing a sliding-scale penalty system based on platform revenue, user base, and level of non-compliance. 2. Verified Parent/Guardian Discretion by introducing a Parental Consent Framework to allow parents/guardians to grant access to age-restricted platforms for children under 1. 3. Government-Endorsed Digital Age Verification System (DAVS) Develop a Digital Age Verification System (DAVS) that verifies user ages anonymously through tokens or hashed data. 4. Strengthened Privacy Protections inc mandated data minimisation practices 5. Non-Monetary Penalties under OSA. 6. Grant Support for Smaller Platforms e.g establish a Small Platform Support Fund to assist platforms with annual global revenue under $5 million AUD in adopting compliant age-verification systems. 7. Education and Awareness Campaigns - Fund national education initiatives to promote: - Digital literacy for children and parents. - Awareness of online safety resources and the amendment's goals. - Collaborate with schools to integrate digital safety into curricula.	We acknowledge the importance of these issues but these are beyond scope of these Codes.
16 UNICEF	1. Strengthen safety and privacy protections for children • Require all platforms to introduce robust default safety settings to reduce risk of exposure to Class 1C and 2 materials, irrespective of whether the service permits Class 1C and 2 materials in their terms of use. • Clearly outline requirement for services to take a data minimisation approach, particularly for age assurance measures which should be proportionate to risk, user-friendly, and handle only personal information essential for service delivery. 2. Ensure strong accountability and transparency mechanisms • Apply risk assessment requirement to all online services, including requirements for companies to mitigate each risk identified and report publicly on how they have assessed and responded to risks. • Clearly define 'a significant number of Australian children' for the purpose of risk assessments, to avoid differential interpretation and application across industries. • Stipulate the need for all services to adopt child-friendly information and tools, including Terms and Conditions (T&Cs), to ensure transparency and accessibility for younger users. 3. Apply a child rights approach • Adopt established guidance on upholding children's rights in digital environments when assessing and mitigating risks for children to ensure the Codes always support the highest level of protection for children possible without unduly limiting their rights. 4. Engage with children and young people • Extend and expand the public consultation on the Draft Industry Codes to undertake genuine and meaningful consultation with children and young people.	In relation to 1. The Codes contain strengthened default settings for children to the extent these are relevant to Class 2/Class1C materials we note that the Children's Privacy Code to be developed by the OAIC will also strengthen children's privacy settings. The requirements to take a data minimisation approach to age assurance is also in the revised Head Terms. 2. Risk assessment and transparency requirements via reporting to eSafety are required under relevant Codes.. These supplement existing ad hoc and periodic reporting in relation to Class1C and Class 2 materials already in force under the BOSE. 3. See updated note to Head Terms clarifying the need to consider children's rights. 4. The Code developers have unfortunately been unable to engage directly with young people due to the tight timeline for Code development but we have had regard to public views expressed by the eSafety Youth Advisory Council.

submission number and name	issue description	Response
17 Relationships Australia	Recommendation 1 The Head Terms, the Codes and their explanatory materials should explicitly state that they are informed by principles of harm minimisation and proportionality of risk (in terms of likelihood of occurrence and gravity of consequences of risk materialisation), as well as a principle of collective responsibility for online safety, which is shared among governments, service providers and end-users, relative to their respective capacities to minimise risk and harm. Recommendation 2 The Codes and explanatory materials should make plainer the distinction between 'high impact classified material' (a concept introduced for Phase 2: see, eg, Head Terms, pp 9-10; Schedule 2, clause 6.1; Discussion Paper, p 50) and 'high priority restricted material (see, eg, Discussion Paper, pp 8, 11, 12, 16). Recommendation 3 To simplify the drafting and make the Codes more accessible, the words 'technically feasible' should be omitted; the requirement that actions be 'reasonably practicable' is sufficient. Recommendation 4 The Codes should expressly require industry participants to take measures to minimise risks of identity theft. Recommendation 5 The Codes (including the Codes already in force) should move away from use of 'Australian' as a descriptor, and refer instead to end-users in Australia who access services or use devices. Recommendation 6 For clarity and simplicity, the Codes and supporting explanatory material should refer consistently to 'parents and carers' of children. Recommendation 7 The Codes should frame obligations using direct and active language. Recommendation 8 The Head Terms should refer to where the relevant practices or fantasies are specified for paragraph (a) of the definition of class 1C material. Recommendation 9 Care should be taken in developing and using facial age estimation measures for the purpose of age assurance systems, to proactively guard against contamination by implicit bias. Recommendation 10 The Schedules and accompanying explanatory materials should provide clear and explicit statements as to the specific contexts in which obligations are imposed in respect of simulated gambling materials. Recommendation 11 Measures such as those set out at Schedule 1, subclauses 7.1.8 and 9.3.2, should be strengthened by requiring industry participants to ensure that means of reporting, flagging or complaining about content are: • not merely provided or published, but actively promoted, to reflect that online safety is a collective responsibility • visible on home pages and online safety information locations established pursuant to provisions such as Schedule 1, sub clause 8.2.16 • culturally sensitive • accessible to people with disability • accessible by children and young people (acknowledging that children and young people are rights-bearers with agency and are entitled to access reporting and complaints mechanisms, in accordance with the Convention on the Rights of the Child and the International Covenant on Civil and Political Rights) • as frictionless as possible (and certainly as frictionless as accessing	1. Noted. The Codes aim to do so, noting it is anticipated that the rolling government privacy reform agenda will deal with privacy concerns to a large extent. 2. There are a range of transparency mechanisms in the Codes including reporting to eSafety. These supplement existing mechanisms in the OSA such as periodic and non periodic reporting under the BOSE. 3. We think it is important to retain the technical feasibility concept which is built into the OSA and Phase 1 Standards. 4. This is not in scope of these Codes. 5. the Codes use the terminology of the Phase 1 Codes and the OSA. 6. We have updated the Codes as requested. 7. We have aimed to do so. 8. This is not a fixed category under the National Classification Scheme. 9. Noted. This is an issue that we hope will be considered in the context of the Age Assurance Trial. 10. Definitions of simulated gambling are drafted to align with the National Classification Scheme. 11. We consider that these issues are best addressed in guidance from eSafety on code and BOSE compliance. 12. What is reasonable will vary based on the complexity of complaints, given much of this content is lawful and requires nuanced judgments under the National Classification Scheme. 13. See response to 11. 14 Considered. 15. Considered. 16. Considered. 18. The Codes aim to do so,

submission number and name	issue description	Response
18 Digital Rights Watch	1.Pause further development until the Codes can be aligned with the government's ongoing reform agenda. 2 Use clear and consistent definitions of Class 1C and Class 2 material 3.Provide a transparent appeals process. 4 Limit the burden of compliance on businesses. There is also a risk that an overly cumbersome burden of compliance will not encourage platforms to create safer environments, but rather restrict access for all users by geography. In the US, where age verification laws have been introduced in several states. Pornhub has blocked access to all users in those states.As reported in The Guardian, users in those states have resorted to using virtual private network (VPN) connections to get around the block.	1. Noted. 2. Codes have been updated to align definitions as far as practical. 3. Complaints can be made to Commissioner for Code breaches if not dealt with in an appropriate manner 4. Noted.
19 Scarlett Alliance	1. Remove the term 'high impact pornography'.as generates stigma for those that create and consume pornography. 2. Remove the term 'seriously harmful material' when referring to class 1C material in the Head Terms para 1.1. 3. Remove '[i]ndustry participants may use different terminology to describe class 1C. 4. Remove 'filtering high-impact online pornography...out of news and discovery feeds. 5. Insert an additional clause in the Head Terms to future-proof the Codes to incorporate amendments to the National Classification Scheme Guidelines. by downlisting, prioritising or quarantining, so that it is not brought to the attention of child end-users' as an example of 'appropriate measures to prevent child end-users from accessing or being exposed to high-impact online pornography or self-harm material' (see e.g. Schedule 1 Social Media Services Online Safety Code, MCM 1.3). and class 2 material for different audiences' (clause 3 (e)) from the Head Terms. 6. Insert an additional clause in the Head Terms recognising the right of adults to participate in lawful sexual expression in online spaces. 7. Include requirements for clear and accessible avenues for challenging malicious or inaccurate reporting under 'reporting and complaints mechanisms' (see e.g. Schedule 1 Social Media Services Online Safety Code, MCM 1.8). 8. Remove the list of 'appropriate age assurance' measures from the Codes Head Terms section 5.1(c)(vi).Head Terms on upholding human rights principles and compliance with state/territory anti-discrimination law.	1. and 2.Definitions relating to pornography have been revised to take into account this feedback. Industry needs certainty about the types of age assurance that can be implemented. 3. is retained so that language e.g in user terms and conditions is user friendly; generally users will not know what Class 2 or Class 1C means. 4. This is retained per feedback from eSafety. 5. The Code can be updated if definintins change (noting this is likely to proceed slowly). 6. This is not a human right protected by Australian law and must be balanced against the potential harm of ponographic materials to children. We have however tried to ensure the principle of proportionality is adopted in the approach to the Code measures. 7. This is out of scope and will likely be covered by future regulatory developments under consideration generally.8. The list has been based on guidance from the UK regulator to help promote regulatory consistency across jurisdictions.
20 Aylo	a device-level and ecosystem-based approach to age assurance is the only effective approach in preserving the online safety of children and other users while also balancing the principles and core values of privacy, data security and freedom of expression. that ecosystem and device-level age assurance methods must be prescribed as the only appropriate or approved age assurance methods that should be implemented by service providers who are subject to the Phase 2 Codes, including Designated Internet Service ("DIS") providers.	We acknowledge these concerns but we do not think it is appropriate to mandate device level assurance for these Codes. See rationale for age assurance in the Request for Registration document.
21 Scarlett Alliance	short version of above	Noted concerns about sex education as a better solution to the policy issues. We have made changes to definitions of pornography in line with this feedback within constraints of the National Classification Scheme.

submission number and name	issue description	Response
22 Scarlett Alliance Sex Worker Project	1.We strongly recommend that the Codes explicitly exclude advertising for in-person sex work services from being classified as class 2 material, and ensure compliance measures do not disproportionately harm sex workers' ability to advertise online. 2. Restricting access to pornography is neither an effective nor a comprehensive solution to preventing harm or improving sexual education for young people. Research consistently shows that age-appropriate, evidence-based sex education is a more effective strategy to equip young people with the tools to navigate online content safely.	see above.

submission number and name	issue description	Response
23 Eros Association	1.We recommend that clause 1.1(a) be amended to delete 'seriously harmful material or' so that its first sentence reads: "The purpose of this Code is to establish appropriate safeguards for the community in relation to certain types of material not suitable for children, referred to in this Code as 'class 1C' and 'class 2' material." 2.We recommend that an additional clause 1.4 be inserted to read: "Industry partners acknowledge the ongoing work on classifications review, namely that the Review of Australian Classification Regulation recommended that legal fetishes be removed from the X18+ (class 1) classification and that the National Classification Code and Classification Guidelines be updated. Where necessary, changes to the classification system will be reflected in future versions of this Code." 3.We recommend that clause 2.1 be amended to delete 'both' and replace 'and' with 'or' so that it reads: "age assurance is an umbrella term for a range of methods for assessing a user's age, including age verification solutions (being solutions that aim to verify the exact age or age range of a given user) or age estimation solutions (being solutions that aim to estimate the exact age or age range of a given user)." 4.We recommend that clause 3(e) be deleted. 5.We recommend that clause 5.1(c)(vi) be deleted. If this clause is not deleted, we will raise our concerns with eSafety. 6. We recommend that clause 5.1(c)(vii) be deleted and that the sentence . We recommend that clauses 1.4 and 1.5 be consolidated to read: "Reporting and complaints mechanism The provider of the service must provide tools which enable Australian end-users to report, flag and/or make a complaint about class 1C and/or class 2 material which they consider may be contrary to a service's terms and conditions and ensure that these reports are considered and actioned appropriately. Such reporting mechanisms must: (a) be easily accessible and easy to use; (b) be accompanied by clear instructions on how to use them; and (c) be available and accessible to Australian end-users on-the interface of the designated internet service. Guidance: In implementing these measures, providers of a designated internet service should ensure that reporting tools are integrated within the functionality of the designated internet service in a manner that is visible and accessible at the point the Australian end-user accesses materials. "in the note after clause 5.1(c)(vii) - "For the avoidance of doubt, compliance with Australian privacy law is not a requirement of this Code." also be deleted. 8. We recommend that clauses 1.7 and 1.14 be consolidated to read: "Training for personnel on online safety The provider of the service must have, or have access to reasonably adequate personnel to oversee the safety of the service. Such personnel must have the skills, experience and qualifications needed to ensure that the provider complies with the	The defintions of pornogarphy have been updated to take into account this feedback. It is not appropriate to refer to reform recommendations for the National Classification Scheme that have not been implemented.

submission number and name	issue description	Response
24	*issue description*	*Response*
25	I'm interested to know what falls under the criteria of "proportionate action" in regards to responding to breaches in rules on a DIS or online service. People can easily make an alternative account, if banning is the most common "proportionate action". Will this action include IP banning? There should be a clear specification of relevant actions that should be taken based on the offences on platforms.	*Response*
26 The App Association	We reiterate concerns raised with Australian policy makers during the development of the Online Safety Act that its requirement for content detection without direct monitoring of private communications raises concerns about the practical implementation and effectiveness of compliance measures, especially for end-to-end encrypted services. The defining feature of end-to-end encryption is that no party other than the sender and the intended recipients, including the service provider, can access the contents. The imposition of a mandate to scan class 1A and 1B material would render it unfeasible for service providers to uphold their commitment to user privacy. It could compromise the fundamental principle of encryption. Moreover, any form of content moderation would likely involve the insertion of a backdoor or a system vulnerability. This could weaken encryption, leading to unauthorised access, exploitation, and surveillance.	Noted.
27 Collective Shout	1. Age assurance processes should be implemented for all online services and Tier 1 and Tier 2 equipment that Australian end-users engage with. 2. Operating system providers and device/equipment providers should be required age estimation technologies to provide the highest level protections for child users. 3. Messaging services should prohibit Class 1C and Class 2 materials and the Codes should require these services to scan/remove these materials. 4. Industry Codes must be technology-neutral to allow for new developments and research to be quickly implemented. 5. Industry Codes require services that prohibit high impact online pornography to still implement age assurance measures to limit the risk of child end-users accessing or being exposed to high impact online pornography.	1. and 2 We have considered this feedback. See request for registration document that outlined the rationale for the approach. 3. The Government has proposed to exempt messaging services from age restrictions under the OSA. The industry does not support scanning of private messaging to remove lawful materials. 4. Agree. We believe that this is achieved by the Codes. 5. This has been addressed by the OSA amendments of November 2024 for age restricted social-media platforms.

submission number and name	issue description	Response
28 Assembly Four	1. Remove age assurance compliance measures completely. 2. Providers of relevant electronic services that allow users under 18 should not be required to scan all Australian user's communications and messages to detect and remove lawful Class 1C and Class 2 materials. 3. Australian end-users who engage with online devices or services should not be required to undergo age assurance processes including Australian end-users who wish to access 'high impact services'.	Noted. We have not required scanning of messaging services.