DIGI submission on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026

Table of Contents

Executive Summary

The Digital Industry Group Inc. (DIGI) thanks the Office of the Australian Information Commissioner (OAIC) for the opportunity to provide our views on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the Exposure Draft) and its Explanatory Statement, released for consultation in March 2026.

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, HelloFresh,

Meta, Microsoft, Pinterest, Snap, Spotify, TikTok, Twitch and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI strongly supports the development of a Children's Online Privacy Code (the Code) (COPC) and welcomes the efforts of the OAIC in this space. Our members have made substantial, sustained investments in children's privacy and safety, and we share the OAIC's commitment to ensuring children's personal information is handled in ways that genuinely serve their best interests.

DIGI recognises that large technology companies are in the spotlight when it comes to questions of data privacy, and are rightly held to a high level of public scrutiny. However, there is a high level of technical experience with data governance in 'digital first' companies; this expertise may not exist to the same extent in other industries that are also using personal information in scope of the COPC. DIGI's relevant members protect young people's privacy online in a wide range of ways, including setting default privacy settings for minors, restricting unwanted contact, limiting advertising to minors, integrating privacy and safety features, offering family controls, and providing data rights for minors and others to access, download, and transfer their personal information.

The central concern of this submission is that a number of these important objectives have been operationalised with an unnecessarily high degree of prescription. As currently drafted, several provisions operate as mandatory compliance requirements rather than principles-based safeguards. This risks increasing personal information collection, including the collection of personal information from parents and carers required to support consent and verification mechanisms, reducing access to important safety and integrity features, and producing consent-heavy user experiences that may ultimately undermine the Code's objectives.

This highly prescriptive approach to the COPC has practical implications for children's ability to use and benefit from online services. Children and young people should be able to enjoy services that are safe, age-appropriate and genuinely useful. DIGI is concerned that unless the current drafting of the Code is recalibrated, children may lose access to features that support their safety and wellbeing, such as technology that ensures age-appropriate experiences. Furthermore, services may be incentivised to collect additional personal information to satisfy age-assurance requirements which is the opposite of the Code's data minimisation objective. In addition, parents and young people may face consent frameworks that are difficult to navigate in practice.

This concern is most clearly illustrated by the interaction of the Exposure Draft's key threshold concepts. The proposed "strictly necessary" standard departs from the established "reasonably necessary" standard under Australian privacy law and, as currently drafted, risks restricting data processing that supports children's safety, service integrity, and age-appropriate experiences. The combined effect of the proposed age-assurance framework, consent architecture, and best interests of the child (BIOC) test applied at each individual data handling step risks producing consent-heavy services and sub-optimal user experiences. Rather than protecting children, this approach may overburden parents, carers and children with consent requests while simultaneously requiring *more* personal information to be collected and delivering *less* functionality and fewer safety protections.

While DIGI strongly supports the policy objectives of the Code, some provisions appear to shift away from the principles-based approach that underpins the Australian Privacy Act 1988 and that informed the design of the UK Age Appropriate Design Code (AADC). We understand that it is the Government's intention that the Code align, where possible, with the AADC. DIGI would suggest the OAIC give further consideration to whether a more principles-based model, closely aligned with the AADC, could achieve the same child safety outcomes with greater regulatory consistency.[1] The AADC is

[1]Australian Government, Government Response to the Privacy Act Review Report (Attorney-General's Department, September 2023) 13, 30. The Australian Government's agreed position on Proposal 16.5 stated: 'to the extent possible, the scope of the

fundamentally a privacy-by-design framework. It seeks to achieve child privacy outcomes through service design, governance measures and risk mitigation, rather than highly prescriptive consent and data-handling requirements. DIGI considers greater alignment with that approach would better achieve the Code's objectives to adopt best practice approaches to the handling of children's personal information while avoiding many of the unintended consequences identified throughout this submission.

DIGI urges the OAIC to reorient the Code around a proportionate, risk-based and privacy-by-design framework with the best interests of the child (BIOC) at its core. Critically, BIOC should serve as an overarching principle informing the design and operation of services as a whole, rather than a transactional test applied at each individual data handling step. The UN Convention on the Rights of the Child (UNCRC) recognises BIOC as a dynamic and holistic concept, one that balances privacy against other fundamental children's rights including identity, expression, association, education and play. A checklist approach does not capture this. Grounding the Code in this broader understanding of BIOC would align Australia with international best practice, including the UK AADC, and produce a framework that is both more principled and more workable across the diverse services the Code covers.

An important corollary of this approach is that, where the Code expands upon existing privacy protections, those measures should deliver a demonstrable privacy benefit for children that is proportionate to the risk addressed, the additional collection of personal information required, and the compliance burden imposed.

The recommendations in this submission are directed towards that outcome. In particular, DIGI recommends:

1. Embedding proportionality and risk-based decision-making directly into the Code's drafting, rather than relying on the Explanatory Statement. (Section 1)
2. Replacing the "strictly necessary" standard with the Australian Privacy Principles (APPs) "reasonably necessary" standard, underpinned by the BIOC as a holistic, overarching framework across the Code, to better accommodate processing that supports children's safety, age-appropriate experiences, and service integrity. Alternatively, the OAIC could model the approach on the UK AADC. (Section 2)
3. Clarifying key threshold concepts including "likely to be accessed by children", "ascertain age", "harm" and the BIOC. (Section 2)
4. Recognising that personalisation, safety processing and certain service-improvement activities can be consistent with children's best interests and, in many cases, are essential to delivering safe and age-appropriate experiences. (Section 2)
5. Avoiding compliance pathways that effectively require system-wide age assurance or the application of very stringent child-focused settings to entire user populations. (Section 2)
6. Reforming Division 2's consent framework to minimise unnecessary collection of personal information and consent fatigue, while preserving meaningful protections for children. (Section 3)
7. Providing a phased implementation period of at least 12–24 months, supported by guidance and continued engagement with industry. (Section 3)

DIGI and its members share a common objective with the OAIC: a Code that delivers strong privacy outcomes for children while remaining proportionate, workable, interoperable and effective in practice. We offer these recommendations in that constructive spirit. We look forward to continued engagement with the OAIC through the Code's development, registration, and implementation. We would particularly welcome targeted follow-up engagement on the issues raised above and would

---

Australian Code will align with the UK Age Appropriate Design Code' <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.

stand ready to coordinate further input from DIGI's members where that would assist the OAIC's deliberations.

Section 1: Overarching considerations

1.1 DIGI's continued support for a Children's Online Privacy Code

1.1.a. DIGI has consistently supported the development of a Children's Online Privacy Code (the Code), including in our submission to the OAIC's July 2025 Issues Paper. We continue to support the OAIC's policy objective of strengthening privacy protections for children, and recognise the importance of giving children, young people, parents and carers confidence that personal information is being handled in a way that is consistent with the best interests of the child.

1.1.b. In DIGI's view, the Code will best serve children's privacy interests by adopting a proportionate, risk-based framework underpinned by in the best interests of the child (BIOC), rather than a prescriptive, rules-based approach. Such a framework would ensure the Code operates consistently with the Australian Privacy Act 1988 (Privacy Act) and established international practice, including the UK Age appropriate Design Code (AADC). Critically, it would also ensure that any additional protections imposed on industry are evidence-based and calibrated to the risks they are designed to address, making the Code more durable, more workable, and more likely to achieve its intended goals.

1.2 The need for greater clarity, proportionality and a risk-based approach

1.2.a. DIGI supports the proportionate, risk-based approach which is articulated in the Explanatory Statement. The difficulty is that this approach does not carry through into the Code's operative provisions, which is where it matters most. As a non-binding interpretive document, the Explanatory Statement cannot fill that gap. DIGI therefore submits that core concepts including proportionality, risk calibration and interoperability should be expressly reflected in the drafting of the Code itself. Throughout this submission, DIGI encourages the OAIC to assess each obligation through an additional risk lens: what additional risk does the measure address beyond the protections already provided by the Privacy Act and Australian Privacy Principles, the Online Safety Act (OSA), the Classification Scheme, Unfair Trading Practices (UTP) reforms, gambling advertising reforms, and existing industry safety and privacy practices. Where the same policy objective can be achieved through less intrusive means, the Code should favour that outcome.

1.1.c. This is particularly important given the breadth of services captured by Section 7. The Code applies to APP entities providing an Social Media Service (SMS), Relevant Electronic Service (RES) or Designated Internet Service (DIS) under the OSA[2] where the service is likely to be accessed by children or primarily concerned with children's activities. These categories capture a diverse range of services with very different risk profiles, user relationships, and levels of child engagement.

1.1.d. By way of illustration the scope of the definition of SMS captures interactions between two or more end-users, including local and small business community forums, educational technology, business forums, health support forums, and any blogs with comments enabled. RES includes email, MMS and SMS services, dating services, gaming services with communications functionality, and messaging services with varying reach and risk

[2] Social Media Service, Relevant Electronic Service, or Designated Internet Service.

profiles. DIS services are even more diverse again, and include operating systems, cloud storage, large language models, and the full gamut of apps and websites used by Australians ranging from basic utility apps that help users find the date or time of day, through to community websites and adult services. Applying the Code's most prescriptive requirements uniformly across this ecosystem risks encouraging broad age-assurance measures, increased collection of personal information and child-oriented settings across entire user populations, including adults, without necessarily delivering proportionately better outcomes for children.

1.1.e. As currently drafted, the provisions relating to "likely to be accessed", age assurance, "strictly necessary" processing and the Division 2 consent framework do not fully reflect the proportionate, risk-based approach described in the Explanatory Statement. In practice, services may be driven toward one of two conservative compliance models:

a. age-assure all users so the Code can be applied only to children; or
b. apply the Code's most restrictive requirements across the entire user base to avoid age determination altogether.

1.1.f. Neither outcome is proportionate. The first risks significant expansion of age and identity data collection, contrary to the Code's data minimisation objectives and the OAIC's own age-assurance guidance. The second risks reducing functionality, personalisation and safety features, particularly for children, by making age-appropriate experiences contingent on consent or age determination. In some cases, services may simply restrict access altogether.

1.1.g. A risk-based, age-graduated approach to online services is independently endorsed from a child-welfare perspective by Internet Matters, which concluded from its May 2026 review of the UK Online Safety Act that children's access to online spaces should be determined by the level of risk a platform presents, not a one-size-fits-all approach.[3] The OAIC's Social Media Minimum Age (SMMA) Privacy Guidance also endorses assessing "*whether the circumstances surrounding the specific chosen method(s) justify the privacy risks*".[4] This concern is developed further in section 2.4 below.

1.1.h. These examples illustrate why the Code's key threshold concepts should be calibrated through a proportionate, risk-based lens and embedded directly within the Code itself.

1.3 Alignment with the Privacy Act and broader privacy reforms

1.3.a. DIGI is concerned that Division 2 may inadvertently require parental consent before under-15s can create an account. Together with the "strictly necessary" threshold and data destruction obligation, this would significantly expand the current Privacy Act framework. DIGI asks that OAIC confirm whether this is an intended outcome and, if not, to amend the drafting to make that clear.

---

[3]Internet Matters, The Online Safety Act: Children's Experiences One Year On (Internet Matters, May 2026) 36: 'Children's access to online spaces should be determined by the level of risk a platform or service presents, and the effectiveness of the safeguards it provides, rather than through blanket bans on categories of platforms. A risk-based approach ensures children can access digital services safely, while preserving opportunities for age-appropriate engagement and learning' <https://www.internetmatters.org/wp-content/uploads/2026/04/Internet-Matters-Online-Safety-Act-Report-May-2026.pdf> (accessed 7 May 2026).

[4]OAIC SMMA Privacy Guidance: Section 3 page 9. Office of the Australian Information Commissioner, Social Media and Minors Age Appropriate Privacy Code Guidance (OAIC, 2025) s 3 (p 9)Australian Government, Government Response to the Privacy Act Review Report (Attorney-General's Department, September 2023) 13, 30. The Australian Government's agreed position on Proposal 16.5 stated: 'to the extent possible, the scope of the Australian Code will align with the UK Age Appropriate Design Code' <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.under-15s <https://www.oaic.gov.au/_data/assets/pdf_file/0025/257146/OAIC-SMMA-Privacy-Guidance.pdf> (accessed 7 May 2026).

1.3.b. As drafted, it is unclear whether Section 10(3) of the Code modifies or supplements the existing fairness requirement in APP 3.5. This underscores our concerns with the drafting approach to the Code more broadly. Attaching BIOC obligations to individual provisions generates interpretive complexity without delivering clearer outcomes for children. This reinforces the need for that BIOC to be repositioned as an overarching principle governing the Code as a whole, rather than embedded in discrete operative provisions.

1.3.c. The OAIC will be aware that the Government has recently signalled an intention to introduce a 'fair and reasonable' test through Privacy Act reform. This illustrates a practical gap in the current drafting. If foundational concepts underpinning the current privacy framework change, the Code's scope could change significantly as a direct consequence, yet there is no mechanism for review or further consideration of the practical impact. DIGI submits that the Code should include an explicit review trigger to address this risk.

1.4 Cumulative consent burden on children, young people, and guardians

1.4.a. DIGI invites the OAIC to consider whether the cumulative weight of the consent provisions is appropriately calibrated to risk, materiality, and the best interests of the child.

1.4.b. For example, a parent/carer with children aged 12 and 14 across five common service categories (e.g., social media, gaming, education, music streaming, and video) faces under the Code as drafted:

- a verified parental consent transaction plus separate child assent at each sign-up;
- annual re-consent on each service's own cycle; and
- per-purpose consent for each material data processing purpose e.g., safety signals feeding into a content safety model

for each individual service. (Detailed further in Appendix A scenario 5.)

1.4.c. Across two children and five service categories, even if each child is only using one service from each service category (for example, one gaming service, or one music streaming service), this produces a minimum of 20 consent obligations, assuming no further data handling for feature use, falling at different points throughout the year. The aggregate creates an obligation parents and carers cannot reliably sustain, and service functions including safety and reliability would degrade if consent or assent is refused or delayed. It is also not clear that each transaction in this chain addresses a harm that could not be achieved by less burdensome means.

Summary of recommendations in Section 1

A. The Code should embed a proportionate, risk-based and privacy-by-design framework, with the BIOC as an overarching principle.

B. Core concepts currently addressed in the Explanatory Statement, including proportionality, risk-of-harm factors for Section 8 age-assurance (pages 6-7), and regulatory consistency, should be reflected in the operative provisions of the Code.

C. Each obligation should be assessed against the additional privacy benefit it delivers beyond existing protections under the Privacy Act, the OSA and established principles, and comparable frameworks and whether that benefit to children is proportionate to the risk, implementation burden, and additional collection of personal information required.

D. The Code should expressly recognise that an effective implementation pathway is one that protects children's data without driving system-wide age assurance or expanded collection across all users both adult and child.

E. The Code's drafting of "lawful" and "fair" should be considered in light of the Government-endorsed "fair and reasonable" test proposed under the Tranche 2 reforms, to avoid unintended consequential reinterpretation of APP 3.5 beyond the children's privacy context.

F. The Code should be subject to explicit review if key Privacy Act provisions are amended through the Tranche 2 reforms, given the potential for consequential expansion of the Code's scope.

G. The Code's success would benefit from the OAIC's targeted consultation with RES, DIS and SMS industry sections, ensuring a cross-section of industry representation.

Section 2: Code drafting and clarity

2.1. Embedding key concepts in the Code would support legal certainty and durability

2.1.a As discussed in Section 1.2, DIGI considers that several substantive concepts currently contained in the Explanatory Statement would benefit from express inclusion in the Code itself. In particular:

i. a proportionality and risk-based principle applicable to all obligations;
ii. the BIOC as an overarching interpretive principle
iii. non-exhaustive factors for the "likely to be accessed by children" assessment;
iv. recognition of a spectrum of approaches to age assurance calibrated to risk;
v. clarification of how features like personalisation, safety processing, and service-improvement activities interact with Section 9's "strictly necessary" threshold; and
vi. the legal basis for re-use of age-assurance data collected for, *inter alia*, SMMA purposes.

2.2. Sections 10 - 11: Best interests of the child (BIOC)

2.2.a. We have long supported the best interests of the child as foundational to the Code, and

continue to do so. However, we recommend that the Code expressly position BIOC as an overarching interpretive framework, consistently with the BIOC under the The UN Convention on the Rights of the Child (UNCRC) and the UK AADC, rather than as a test at every individual data handling step. In this way, the BIOC would inform the application of the Code as a whole, recognising that children's rights under the UNCRC, including privacy and protection alongside participation, education, play and access to information, must be considered holistically.[5]

2.2.b. As currently drafted, however, the Code applies BIOC at the level of individual data-handling activities, requiring each collection, use or disclosure of personal information be in the child's best interests. DIGI is concerned this approach may discourage ordinary, low-risk processing that supports safe, age-appropriate and functional digital experiences for children and young people.

2.2.c. This differs from the approach adopted in the UK AADC, regarded for example by digital children's rights organisation 5rights, as a leading international framework for children's privacy, and provides a useful reference point when considering how similar concepts in the Code drafting have been operationalised.[6] The AADC's approach is also more consistent with the UNCRC's treatment of best interests as a context-dependent assessment that balances multiple rights and interests, and reduces the risk of unintended outcomes, including the withdrawal of functionality that may genuinely support children's interests. DIGI's view is that BIOC, properly understood, requires digital services to actively promote children's wellbeing - not merely to refrain from causing harm. This distinction matters: a BIOC-framed Code should require services to ask what a child-friendly service looks like by design, not simply individual data practices in isolation.

2.3. Section 7: Scope - services "likely to be accessed by children"

2.3.a. DIGI's position is that, as currently drafted, the "likely to be accessed by children" threshold risks capturing any service children are theoretically capable of accessing, without applying a meaningful proportionality filter. Absent further clarification of the drafting, the "likely" sets a low threshold that would extend Code obligations to services never designed for, directed at, or materially used by children, thus significantly over-capturing services and imposing compliance burdens with no corresponding child protection benefit (see for example Appendix A Scenario 1). DIGI recommends adjusting this threshold to ensure there is a more tangible nexus between a child accessing a service and risk of harm. We believe this can be achieved by having regard to the nature, design and purpose of the service (specific factors are outlined below). This is consistent with the UK Information Commissioner's Office (ICO) guidance on the AADC, which recognises that incidental child access does not, of itself, bring a service within scope.[7]

2.3.b. Access threshold and proportionality: The UK ICO's guidance on the UK AADC provides a sound backdrop to how a service is 'likely' to be accessed by children where children use it in reality, rather than where they could theoretically do so. The ICO highlights that services that are adult-only or otherwise child-inappropriate should focus on avoiding child access rather

[5] UN Committee on the Rights of the Child, General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2 March 2021) paras 12–13, <https://digitallibrary.un.org/record/3906061> (accessed 12 May 2026).
[6] 5Rights Foundation, 'Celebrating 3 Years of the Age Appropriate Design Code' (Blog Post, 2 September 2024) <https://5rightsfoundation.com/celebrating-3-years-of-the-age-appropriate-design-code/> (accessed 4 June 2026).
[7] Information Commissioner's Office (UK), 'Likely to be accessed by children' (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/> (accessed 26 May 2026).

than becoming child-friendly by default by virtue of the Code's application.[8] Our position aligns with this approach and consequentially, where a service becomes reasonably aware of underage access and takes reasonable steps to remove that child, it should not be found in breach of the threshold by reason of that incidental access alone. Rather, compliance should be measured by proactive design and reactive responsiveness, not by isolated underage access events. DIGI recommends these principles be codified to give regulated entities a clear and principled basis for the threshold assessment, particularly given the breadth of services and downstream compliance obligations including age-appropriate data handling and safety processing that should not be undermined by threshold uncertainty.

Non-exhaustive factors for the assessment

2.3.c. DIGI suggests that the non-exhaustive factors drawing on UK ICO guidance may include:

i. the purpose and design of the service (including whether it is directed to or intended to appeal to children);
ii. the nature of the content;
iii. any age-related access restrictions or terms of service;
iv. the entity's reasonable inferences from existing user data;
v. risk indicators of child access notwithstanding access restrictions;
vi. the reasonable steps taken upon becoming aware of a child on the service; and
vii. the entity's wider regulatory context (including any other age assurance such as SMMA compliance measures the entity has already taken).

Codifying these factors would give regulated entities a clear, principled basis for their assessment.

SMMA interaction

2.3.d. Ensuring the Children's Online Privacy Code and the SMMA framework operate coherently is in the interests of both regulators and industry. DIGI submits that services which have taken reasonable steps to prevent access by under-16 users in accordance with the SMMA regime should not be treated as "likely to be accessed" by children below that age for the purposes of the Code. Where an Age Restricted Social Media service has made genuine efforts to comply, incidental access by underage users should not automatically trigger the Code's full obligations. In those circumstances, the Code should apply only to those users of the service aged 16 to 17, ensuring protections remain targeted and proportionate.

2.3.e. DIGI also encourages the OAIC and eSafety Commissioner to develop joint guidance on the interaction between the COPC and SMMA frameworks to provide greater certainty and promote consistency across both regimes.[9]

2.4. Section 8: Ascertaining the age of end-users

2.4.a. DIGI strongly supports a proportionate, risk-based approach requiring 'reasonable steps' to age assurance consistent with international frameworks. Absent further clarification, the current drafting risks producing outcomes the OAIC seeks to avoid, such as excessive data collection and digital exclusion. The least privacy-intrusive method capable of addressing the identified risk should generally be preferred. This section also addresses a potential legal conflict between the Code and the SMMA framework on re-use of age-assurance data.

[8] Information Commissioner's Office (UK), 'Likely to be accessed by children', above n 7.
[9] The same principle may also be relevant for other regulatory or statutory frameworks that require services/entities to take reasonable steps to prevent access or registration by users below specific ages.

"Ascertain age" should permit a spectrum of assessments

2.4.b. Sections 8(1) and 8(3) appear to require services to determine the actual age of users, potentially implying age verification practices. However, distinguishing a child from an adult is materially different from distinguishing between adjacent age cohorts, such as 14-, 15- and 16-year-olds. The Government's Age Assurance Technology Trial found that age-estimation technologies require buffer zones around age thresholds to manage uncertainty, raising practical questions as to how entities are expected to distinguish between users who sit close to the relevant threshold using current technologies.[10] DIGI therefore recommends that the Code expressly recognise a spectrum of age-assurance approaches, calibrated to the risk of harm, nature of the service and age threshold being assessed, and prioritising lower-friction, less privacy-intrusive methods where appropriate.

2.4.c. This flexibility is particularly important given the growing number of Australian regulatory frameworks that rely on different age thresholds, including under-15, under-16 and under-18 cohorts. Without a coordinated approach, services may be required to undertake additional age-assurance activity and collect more personal information than is necessary to comply with overlapping obligations. The Code should therefore accommodate a range of proportionate methods, including self-declaration, age estimation, behavioural or contextual signals, AI-assisted assessment and age verification where appropriate. This would align with international approaches, the OAIC's age assurance guidance, the OSA Phase 2 Age Restricted Material (ARM) Codes and the findings of the Age Assurance Technology Trial. Consistency across frameworks is essential to avoid fragmented compliance approaches, duplicated infrastructure and unnecessary collection of personal information without corresponding benefits for children.

The meaning of 'harm'

2.4.d. The Exposure Draft does not define "harm" for the purposes of the age-assurance obligation in Section 8(2), despite the level of age certainty required being contingent on the risk of harm identified for handling data. This creates uncertainty as to the circumstances in which more intrusive forms of age assurance may be expected. Consistent with the UK AADC's risk-based approach,[11] DIGI recommends that the Code define "harm" to a child as an adverse impact on the child's fundamental rights and interests. Critically, this assessment should be made holistically, weighing factors including the child's wellbeing, access to information, digital literacy, development, dignity and online freedoms. This approach is consistent with, and grounded in, the BIOC framework. This would provide a clearer and more principled basis for calibrating age-assurance measures, while reducing incentives for disproportionate age-verification practices that may themselves create privacy and security risks.

A proportionate, privacy-preserving approach consistent with international principles

2.4.e. Expressly supporting privacy preserving age signals, including behavioural and contextual

[10] The Age Assurance Technology Trial found that age-estimation systems operate probabilistically and require the use of buffer zones around age thresholds to manage uncertainty. Consistent with the Trial's findings, distinguishing between adjacent age cohorts (for example, 14- and 15-year-olds) is materially more challenging than assessing whether a user is likely to be above or below a broader threshold. Age Check Certification Scheme, *Age Assurance Technology Trial – Part D: Age Estimation* (Australian Government, August 2025) [D.2.3], [D.2.10], [D.9.2]–[D.9.5] Accessed 7 May <https://ageassurance.com.au/report/>

[11] Information Commissioner's Office (UK), Age Appropriate Design: A Code of Practice for Online Services (ICO), Standard 6 ('Age appropriate application'): 'Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing' (or apply the standards in the AADC to all your users instead) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/> (accessed 15 May 2026).

indicators where proportionate to the risk being addressed,[12] would better align with the Code's data minimisation objectives and reduce the need to collect and retain sensitive identity information at scale, avoiding the creation of 'honeypots' of personal information on a wide range of websites (noting the aforementioned broad scope of the DIS, RES and SMS categories) that may themselves create significant privacy and security risks.[13]

Workable implementation of Section 8(5)

2.4.f. Clarification is needed as to how Section 8(5) operates for general-audience services (see Appendix A, for illustrative examples).[14] Several requirements of the Code will produce outcomes appear disproportionate to the additional privacy benefit achieved, including for services with overwhelmingly, if not exclusively adult user bases, including:

i. the consent framework in Division 2;
ii. the destruction right in Section 32; and
iii. the transparency requirements in Sections 23, 24 and 33 (as discussed elsewhere in this submission).

The SMMA age-data re-use legal problem (Section 8(6))

2.4.g. DIGI recommends clarification in the Code of how the COPC and SMMA frameworks are intended to interact where age assurance obligations arise under both regimes, and explore a coordinated amendment in Part 4A of the OSA.

2.4.h. The Explanatory Statement contemplates that age-assurance data collected for SMMA purposes may be re-used for the Code. However, the SMMA framework restricts the use and disclosure of age-assurance data collected for SMMA purposes for other purposes (except in limited circumstances) and requires that such data be destroyed when no longer required.[15] Section 8(6) further provides that nothing in the Code affects another Commonwealth law, creating uncertainty as to whether re-use is permitted in practice. Absent clarification, entities may be required to collect age-assurance information multiple times for overlapping regulatory purposes, contrary to data minimisation principles and the Code's objectives. Requiring separate consent to re-use age-assurance data would also introduce unnecessary user friction and contribute to consent fatigue without an apparent privacy benefit. DIGI therefore encourages a coordinated approach that allows entities to rely on existing age-assurance signals, including age ranges or equivalent outputs, rather than requiring duplicative collection across regulatory frameworks.

2.5. Section 9: The "strictly necessary" default

2.5.a. DIGI's primary recommendation is adoption of the 'reasonably necessary' standard under a holistic BIOC framework, consistent with the APPs and the UK AADC. To be workable, any eventual framing should cover processing reasonably required to:

---

[12] Such as platform-level Declared Age Range APIs as privacy-preserving frameworks that allow apps to determine a user's age category without accessing their exact birthdate, zero-knowledge proofs, age-estimation tools. Note: these are suggested as examples that could be explored as part of a scale of options, rather than endorsements.

[13] Josh Taylor, 'Online age-verification system could create "honeypot" of personal data and pornography-viewing habits, privacy groups warn', *The Guardian* (31 October 2022) <https://www.theguardian.com/technology/2022/oct/31/online-age-verification-system-could-create-honeypot-of-personal-data-and-pornography-viewing-habits-privacy-groups-warn> (accessed 15 May 2026).

[14] Section 8(5): 'This section does not apply if the entity applies this Code, other than this section, in relation to the entity's service regardless of the age of end-users of the service.'

[15] Online Safety Act 2021 (Cth) s 63F(3): 'If an entity holds personal information about an individual that was collected for the purpose of, or for purposes including the purpose of, taking reasonable steps to prevent age-restricted users having accounts with an age-restricted social media platform, then: (a) the entity must destroy the information after using or disclosing it for the purposes for which it was collected…'

i. provide age-appropriate experiences and content;
ii. operate safety, integrity, anti-abuse and anti-grooming systems and to enable parental and teen controls;
iii. maintain security;
iv. support service-improvement activities that materially contribute to safety or age appropriateness;
v. comply with concurrent obligations under the Online Safety Act, Gambling reforms, and other relevant regulatory frameworks; and
vi. operate the features that underpin the uniqueness, relevance, and enjoyment of the service, including personalisation.

2.5.b. The current drafting creates significant uncertainty for these activities. Personalisation, safety processing and certain service-improvement activities are integral to age-appropriate digital services, yet it is unclear whether they would be considered "strictly necessary" under Section 9. As currently drafted, the "strictly necessary" standard would have unintended consequences that would restrict processing that supports children's safety, age-appropriate experiences, service integrity and compliance with other legal obligations. This creates uncertainty for processing that is often central to child safety rather than peripheral to service delivery. For example, a discovery service without age-informed personalisation may surface adult or irrelevant content to children, while a chatbot or interactive platform without behavioural safety signals may be unable to operate effective real-time harm detection systems (see for example Appendix A Scenario 2). Similarly, compliance with concurrent obligations under the OSA Phase 2 ARM Codes may require forms of processing that a narrow reading of Section 9 could restrict.

2.5.c. In practice, a narrow interpretation risks creating fragmented, complex consent-heavy services and preventing the very processing that helps keep children safe online. This approach builds on the Privacy Act's well-established principles to uplift existing privacy protections with youth considerations, rather than introducing new concepts which risk introducing regulatory complexity and uncertainty. As an alternative, the OAIC could look to the UK AADC, which incorporates similar considerations in a flexible and principle-based way.

How personalisation, safety processing, and service improvement as 'strictly necessary' sit under the current drafting

2.5.d. Section 9(1) requires that, by default, entities only collect, use or disclose personal information about a child that is strictly necessary to provide the entity's service. The Explanatory Statement (page 8) indicates that personalised recommendations, targeted advertising and service improvements would not generally be "strictly necessary". Given the scale of services in scope, this risks severely degrading user experiences, inhibiting age-appropriate functionality, and colliding with concurrent online safety obligations.[16]

2.5.e. For example, compliance with the OSA's Phase 2 ARM SMS Code requires AI chatbot services to conduct real-time analysis of conversations to detect self-harm ideation signals, and escalate/respond accordingly (see for example Appendix A Scenario 4). This necessarily involves processing the substantive content of what may be a child's most sensitive personal

[16]For example, in the context of a social media service with messaging and chatbot functionality, the OSA Phase 2 ARM Codes can require services to identify or infer which users are children in order to apply age-appropriate protections and defaults. In practice, this may involve the use of behavioural, contextual (e.g., preferences), and account-based signals and inferences. Section 9's "strictly necessary" standard is in tension with these obligations, as processing these signals across a service falls short of the strictly necessary standard as drafted to provide messaging or social features alone. A strict interpretation of Section 9 therefore creates uncertainty as to whether services may continue to rely on inference-based approaches to identify child users, risking platforms making the choice between blanket child-safe defaults for the entire user base, or formal age verification for the entire user base.

communications. However, under a strict reading of section 9(1), such processing would be difficult to characterise as “strictly necessary” to provide the chatbot service itself. This illustrates the tension between the COPC’s “strictly necessary” threshold and other Australian regulatory regimes that require proactive and/or proportionate safety-by-design measures.

2.5.f. This also illustrates a deeper structural problem: where consent can be withheld or withdrawn, making safety-protective processing contingent on it directly undermines the protective purpose of the Code. Safety and integrity processing, such as detecting grooming, self-harm ideation or at-risk behaviour, should not depend on individual consent as a legal basis. The effectiveness of these protections often relies on their ability to operate regardless of whether consent has been obtained or maintained.

2.5.g. DIGI recommends that Section 9 be amended to address the risk that processing integral to children's safety and service delivery – including self-harm detection, anti-grooming, and age-appropriate personalisation – may be characterised as not 'strictly necessary' and disabled by default.

Alternative approach: the UK AADC

2.5.h. As an alternative, the OAIC could look to the United Kingdom's Age Appropriate Design Code (AADC). While the AADC uses the concept of processing that is "strictly necessary", it does so within a broader privacy-by-design framework that incorporates the BIOC principle, risk assessments, proportionality and the UK GDPR's lawful-bases architecture. As a result, necessity is assessed in context, rather than operating as a standalone restriction on individual data-handling activities.[17] This approach better accommodates processing that supports safety, service integrity and age-appropriate experiences, while maintaining strong privacy protections for children.

Personalisation as safety and meeting expectations of the product: concrete examples

2.5.i. For many services, personalisation is integral to delivering safe, age-appropriate and functional experiences for both children and adults. DIGI recommends that the Code recognise that certain forms of contextualisation and personalisation may support the best interests of the child. Illustrative examples:

- i Search and discovery. A child seeking relationship advice via a web browser may be served adult dating platforms or pages if the service lacks age-informed personalisation.
- ii Relevant content surfacing on a digital-discovery service. Where a service’s core function is surfacing inspiring, educational, or creative content, age-informed personalisation helps ensure children receive relevant and age-appropriate results. For example, a 15-year-old searching for room décor ideas would reasonably expect relevant interior inspiration, rather than unrelated content such as cake decorating tutorials. (For a further example, see Appendix A Scenario 3.)
- iii Real-time harm identification. Behavioural and content signals are used to identify children at risk of self-harm, eating disorders, radicalisation or other harms, and to surface crisis resources. A consent framework that switches off these signals for non consenting users would sit those children outside harm-detection systems at the moment they matter most.

[17] Information Commissioner's Office (UK), Age Appropriate Design: A Code of Practice for Online Services, above n 11 (Standards 1, 6, 7 and 12); Information Commissioner's Office (UK), ‘What Is the Legitimate Interests Basis?’ (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/> (accessed 15 May 2026).

Targeted advertising

2.5.j. DIGI confirms its earlier views that, to the extent the COPC restricts targeted advertising to children, those restrictions should be calibrated consistently with analogous Australian regulatory frameworks, including broadcasting advertising restrictions, to support regulatory coherence and avoid creating inconsistent obligations across sectors.[18] (Further explored in Section 3, 'direct marketing'.)

2.6. Section 13: Age of consent

2.6.a. Section 13 introduces a consent age of 15. DIGI supports additional protections for younger children but notes that this threshold will operate alongside other Australian age-based obligations and existing product practices. The interaction of these frameworks should be carefully considered to avoid complexity, additional age-assurance requirements and increased collection of personal information.

2.6.b. In practice, some services may need to distinguish between multiple age cohorts under Australian law, including users under 13, under 16 and under 18. This risks increasing age-assurance activity in ways that may be inconsistent with the Code's data minimisation objectives. DIGI therefore encourages further consideration of how the proposed threshold interacts with adjacent regulatory frameworks and the practical implications of introducing a unique age threshold with age assurance requirements under the Code.

2.6.c. If the age of 15 is retained, DIGI requests clear guidance on how entities are expected to operationalise the threshold where granular age verification has not been undertaken, particularly given the findings of the Age Assurance Technology Trial regarding the challenges of distinguishing between age cohorts (such as 14- and 15-year-olds).[19]

[18] Digital Industry Group Inc, *Submission to the OAIC Children's Online Privacy Code Issues Paper* (31 July 2025) paras 3.1–3.2 <https://www.oaic.gov.au/__data/assets/pdf_file/0030/255954/Digital-Industry-Group-Inc.PDF> (accessed 15 May 2026).

[19] The Age Assurance Technology Trial found that age-estimation systems operate probabilistically and require the use of buffer zones around age thresholds to manage uncertainty. Consistent with the Trial's findings, distinguishing between adjacent age cohorts (for example, 14- and 15-year-olds) is materially more challenging than assessing whether a user is likely to be above or below a broader threshold.Age Check Certification Scheme, *Age Assurance Technology Trial – Part D: Age Estimation* (Australian Government, August 2025) [D.2.3], [D.2.10], [D.9.2]–[D.9.5] <https://ageassurance.com.au/report/> (accessed 7 May 2026).

Summary of recommendations in Section 2

H. Elevate key substantive concepts from the Explanatory Statement into the Code itself, including:
    a. Including an express proportionality principle to ensure obligations are interpreted and applied in a way that is risk-based, technically feasible and proportionate to the nature of the service, the processing activity and the likely risks to children.
    b. Embedding the best interests of the child as an overarching interpretive standard, with relevant BIOC factors included in the Code itself, consistent with the approach taken in the UK Age Appropriate Design Code.
    c. Clarifying key threshold concepts through non-exhaustive definitions, to provide regulated entities with greater certainty while preserving flexibility for different service types, user contexts and risk profiles.
    d. Recognising a spectrum of age-assurance approaches, rather than implying that one method is required or preferred, to allow services to adopt privacy-preserving and proportionate approaches appropriate to their risk profile.
    e. Clarify the legal basis for re-use of age-related information collected or inferred for compliance with SMMA or other regulatory frameworks, so that entities are not required to repeat age-assurance activities for overlapping obligations.

I. Section 7 — "likely to be accessed by children":
    a. Codify non-exhaustive assessment factors, drawing on UK ICO guidance, including the nature, design, purpose, content and intended audience of the service.
    b. Include a 'directed at' carve-out: services that are not directed to or marketed to children and that take reasonable steps to prevent child access, should not be considered "likely to be accessed by children" by reason of incidental access alone.
    c. Clarify that services taking reasonable steps under other regulatory frameworks to prevent access by users below a specified age should not, by virtue of those steps alone, be deemed likely to be accessed by those users.
    d. Develop joint OAIC/eSafety guidance on the COPC/SMMA interaction.

J. Section 8 — ascertaining the age of end-users:
    a. Expressly provide for a risk-based, proportionate approach, and for a spectrum of age-assurance approaches (self-declaration, estimation, behavioural inference, formal verification) calibrated to the risk of identifiable harm.
    b. Expressly support privacy-preserving age signals and recognise the proportionate, anonymity-respecting design.
    c. Support privacy-preserving age signals and anonymity-respecting design.
    d. Articulate or clarify relevant risk-of-harm factors, including the privacy and cybersecurity risks of age-assurance infrastructure itself.
    e. Allow entities to rely on age signals already collected or generated under other regulatory frameworks, including SMMA, to avoid duplicative collection and verification processes.
    f. Ensure Section 8(5) is risk-based and proportionate, including for general-audience services.

K. Section 9 — “strictly necessary” default:
    a. Replace “strictly necessary” with the APP “reasonably necessary” standard, underpinned by BIOC as a holistic framing across the Code. Alternatively, align the provision more closely with the UK AADC approach.
    b. Expressly recognise processing required for the core operation of a service as "strictly necessary", including age-appropriate experiences, safety and integrity systems, security measures, safety-related service improvements, parental and teen controls, and functionality that supports the child's experience.
    c. Clarify that processing required to comply with concurrent legal obligations, including safety obligations under the Online Safety Act and other Commonwealth laws, is "strictly necessary" for the purposes of section 9, to avoid conflicting regulatory outcomes.
L. Sections 10–11 — Best interests of the child:
    a. Reframe BIOC as an overarching interpretive principle applied across the Code, rather than as a transactional test at each individual data-handling step.
    b. Codify the material BIOC factors from the Explanatory Statement in the Code itself.
M. Section 13 — age of consent:
    a. Ensure the age threshold is interoperable and consistent with adjacent regulatory frameworks.
    b. We welcome continued engagement with the OAIC on the policy rationale for, and practical implications of, any age threshold.

Section 3: Regulatory coherence and compliance complexity

Several requirements in the Exposure Draft risk requiring additional collection and processing of personal information, while creating significant compliance and user friction without clearly delivering proportionate privacy benefits for children. This section focuses on four areas of particular concern: the Division 2 consent framework (including double consent and annual renewal), transparency obligations (Sections 23, 24 and 33), the destruction right (Section 32), and the public Privacy Impact Assessment (PIA) register (Section 39). As DIGI supports the policy objectives underpinning these provisions, we propose targeted adjustments that would better balance privacy outcomes, operational practicality and data minimisation.

DIGI has also consistently supported measures that empower children and families to make informed privacy choices. At the same time, obligations that rely on consent, verification or additional data collection should deliver a clear and demonstrable benefit for children that is proportionate to the additional collection of personal information and complexity of requirements to comply with them.

3.1 Division 2, consent framework: A proportionate alternative

3.1.a DIGI is concerned that the Division 2 consent framework departs significantly from the Privacy Act 1988 and introduces a novel regulatory architecture without corresponding benefits. DIGI supports children having meaningful agency over their personal information, consistent with their evolving capacity and maturity. In our view, this objective is better achieved through a principles-based approach grounded in the Privacy Act, and aligned with the UK AADC as the Government expressly contemplated. Both frameworks reflect a

risk-proportionate model that places the primary obligation on platforms to design services in children's best interests, rather than on families to navigate prescriptive consent transactions. DIGI's view is that the BIOC framework should be applied holistically across the Code rather than transactionally at the level of individual data-handling activities; we consider that this would achieve the same protective objectives without the complexity of the current consent architecture.

3.1.b Under the proposed framework, parents and children may be required to navigate initial consent, separate child assent, annual renewal, purpose-specific consent transactions, and parental verification requirements across multiple services and devices. In contrast, the Privacy Act does not require consent as the basis for all personal information handling; it takes a risk-proportionate approach under which lawful collection is determined contextually. The UK AADC similarly emphasises privacy-by-design and platform-level obligations rather than transactional consent flows. The Division 2 framework introduces novel obligations, including annual consent renewal, purpose-specific child assent, and verifiable parental consent, that are not found in either comparator framework. In DIGI's view, these requirements risk imposing substantial burdens on services without delivering commensurate privacy outcomes for children (see for example Appendix A Scenario 5). DIGI would welcome further information from the OAIC on why these mechanisms and why they are considered necessary to achieve the Code's objectives. The Privacy Act Review Report itself cautioned that "[a]n over-reliance on notice and consent can place an unrealistic burden on individuals to understand the risks of complicated information handling practices and may not result in improved privacy outcomes",[20] which is a risk this framework carries at scale.

3.1.c In DIGI's view the consent model in the current draft risks undermining the very outcomes the Code is designed to achieve. Consent fatigue, barriers to access for vulnerable children, and the degradation of safety features while consent processes are navigated are predictable and well-documented consequences of transactional consent frameworks. DIGI's preferred approach addresses these risks directly. By adopting BIOC as an overarching principle, the onus falls on platforms to demonstrate that their data practices genuinely serve children's best interests. This is a higher and more meaningful standard than consent. It is also consistent with how the UK AADC operates in practice, providing a proven model that Australia can draw on with confidence.

3.1.d DIGI draws the OAIC's attention to its Public Consultation Report (November 2025), which highlights that consent cannot meaningfully improve privacy outcomes where families have little real choice, which is a concern particularly acute in educational contexts.[21] The annual renewal requirement further compounds this risk. It is a novel concept not reflected in comparable frameworks such as the UK AADC (which does not mandate fixed-period renewal) or the Australian Privacy Act (which focuses on whether consent remains current[22]). Research consistently indicates that beyond a certain threshold, additional consent requests

---

[20] Attorney-General's Department, Privacy Act Review Report (Attorney-General's Department, February 2023) 3 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[21] *"...in any situation where a parent is asked to provide consent for their child to use software in a school there is a power imbalance that negated truly independent decision making. The emphasis should instead be on minimum, mandatory privacy controls so that parents and children are alleviated from the burden of having to think about it, in the same way that parents do not have to think about whether the school's art or sports equipment is fit for purpose."* Office of the Australian Information Commissioner, *Children's Online Privacy Code Public Consultation Report (OAIC, November 2025) (response to Question 2 for adults):* https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code-public-consultation-report> (accessed 15 May 2026).

[22] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services,* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/ above n 11 (not containing any requirement for fixed annual consent renewal); Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines (OAIC) ch B (consent must be voluntary, informed, current, specific and given by a person with capacity, and must be capable of withdrawal).

do not improve decision quality and may instead lead to disengagement or reflexive acceptance.[23] Internet Matters has similarly observed that many parents already find it challenging to manage children's online safety settings across multiple services.[24] These realities should inform the calibration of the consent framework.

3.1.e The consequences are not limited to user experience. Verifiable parental consent may be an effective and privacy-preserving method for some services, but should not be treated as universally appropriate. In some contexts, verifying parental or guardian status may require additional personal information or documentation, and may not account for diverse family structures, legal guardianship arrangements, or circumstances where a teenager needs confidential access to support, assistance or health information. This is particularly important where a minor's relationship with their parent or guardian is constrained, unsafe or otherwise unable to support independent access to essential digital services. As UNICEF has noted,[25] age assurance processes should not inadvertently discriminate against children who lack official documents, have developmental delays, are not accurately recognised by algorithmic systems, or do not have parents or caregivers able to participate in verification processes.[26]

3.1.f The framework may also require repeated collection and verification of age, parental status and consent preferences over time, increasing the amount of personal information processed in order to comply with a Code intended to minimise it. DIGI therefore encourages the OAIC to recalibrate the Division 2 framework through a proportionality lens.

Parental/carer verification requirement

3.1.g The Code's requirement to take "reasonable steps" to confirm that consent is provided by a person with parental responsibility (Section 8(3)) raises significant practical and privacy challenges. In many cases, parental or carer verification may require collection of additional sensitive information (such as birth certificates or Medicare cards), particularly where children live in blended families, kinship care arrangements, or other non-traditional caregiving settings.

3.1.h Further, the current drafting does not address how verifiable consent will work in practice, including whether services will be required to build their own verification technology, what accuracy standards will apply.

3.1.i The current drafting to take 'reasonable steps' to confirm that consent is given by a person with parental responsibility (Section 8(3)) also provides limited clarity on how verifiable parental consent is intended to operate in practice. It remains unclear what verification methods are contemplated, what level of assurance is expected, whether common verification services may be relied upon, or what standards will apply. DIGI recommends that any guidance adopt a risk-based approach consistent with age assurance requirements more broadly and recognise that currently contemplated methods may either be highly susceptible to fraud or require collection of intrusive personal information such as government-issued identification or financial credentials.

---

[23] European Commission, *Discussion Paper for Stakeholders' Roundtable on Cookies* (European Commission, 2023) 1: 'may simply give up trying to express their real privacy preferences' <https://commission.europa.eu/system/files/2023-04/Discussion%20paper%20for%20stakeholders%27%20roundtable%20on%20cookies.pdf >.

[24] Internet Matters, *The Online Safety Act: Children's Experiences One Year On*, above n 3, 33: 'Parents also described difficulty keeping up with the different tools available to help manage their children's online experience.'

[25] UNICEF, *Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper* (UNICEF, 2021) <https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pd>

[26] This is consistent with DIGI's 2025 submission: Digital Industry Group Inc, *Submission to the OAIC Children's Online Privacy Code Issues Paper*, above n 18, paras 6.4–6.6.

3.1.j DIGI also suggests that if the parental/carer consent is retained, the concept of "assent" should be replaced with "notice" for younger children, recognising that young children may not meaningfully understand what they are being asked to "assent" to in practice.

Defining direct marketing

3.1.k The Code should clarify that 'direct marketing' under Section 29 does not extend to targeted advertising. Defining the two concepts interchangeably would be inconsistent with the Attorney-General's recommendations on Privacy Act reform, which draw a clear distinction between them, and would represent an unwarranted expansion of the term beyond its established meaning. The practical consequences of such an expansion would be significant. Many services that children rely on are provided free of charge on the basis of an advertising model. Capturing targeted advertising within the definition of direct marketing would undermine the viability of these services without a clear privacy justification. DIGI also submits that targeted advertising, when used appropriately, supports the delivery of age-appropriate content and services to children and is consistent with their best interests. The Code should recognise this rather than treat targeted advertising as inherently contrary to children's privacy

3.1.l Additionally, we are concerned that the Explanatory Notes could be read as requiring both parental consent and child assent for a service to communicate with a child about its own features and functionality, including safety tools, safety notifications, product updates or account-related information. To prevent this operationally impractical dual-consent model from disrupting routine user interactions, DIGI recommends clarifying that first-party service communications are distinct from third-party commercial advertising and are not intended to be subject to the same heightened requirements as the current consent framework.

Implementation for global services

3.1.m Industry needs clarity on how the COPC's consent framework will operate for global services already built around the UK's cookie-consent model. For global services, these requirements may sit alongside existing consent and privacy frameworks, creating additional complexity and friction within a single user journey.

3.2 Consistency with domestic and international frameworks

3.2.a. DIGI recommends that the Code be drafted (and accompanying guidance as necessary) to achieve consistency with the key frameworks already shaping industry practice globally, predominantly the UK AADC, as well as the EU GDPR (see table below) and with concurrent domestic obligations under the OSA, gambling advertising, scams prevention, the UTP Bill notification requirements, Tranche 2, and classification reforms. Where the Code diverges from these frameworks, the Exposure Draft should explain why that divergence is necessary to achieve a materially different policy outcome. Greater alignment enables reuse of existing safety infrastructure, consistent user experiences, and reduced duplicative consent flows. This includes greater alignment with the AADC's privacy-by-design approach, which seeks to achieve child privacy outcomes through service design and risk mitigation rather than reliance on prescriptive consent and data-handling requirements alone. Reliability and consistency facilitate operability and compliance.

Comparison to the UK and the EU

3.2.b. The Government expressly contemplated alignment with the UK AADC where possible, making it an important comparator when assessing how similar policy objectives can be

operationalised.[27] While the policy intent has been to align the COPC with comparable international frameworks including the UK AADC, in our read, the draft Code introduces several novel concepts, rights and approaches not found in the Australian Privacy Principles or aligned with comparable international jurisdictions, and it is unclear why these are necessary to achieve the COPC aims relative to the compliance lift to be placed on almost all online services in Australia.

Model type	COPC exposure draft	UK AADC	EU GDPR
Consent model	Consent-basis Predominantly consent-only framework: no alternative legal bases for processing	Flexible Not a consent-based regime: operates within GDPR's multi-legal basis architecture; legitimate interests available subject to safeguards	Flexible Multi-legal basis architecture (Art. 6): consent is one of several lawful bases including legitimate interests
Parental consent + child agency	Double-consent Two independent actions required: verifiable parental consent plus separate child assent, and neither can be bundled	N/A No equivalent double-consent construct: age-appropriate design obligations do not require parental consent as a condition of processing	Simpler Art. 8 requires VPC below the digital age of consent (varies between 13-16), treated as a single delegated decision under UNCRC Art. 5, not a dual-consent transaction
Consent renewal	Annual renewals Annual renewal required: both parental consent and child assent must be re-obtained every 12 months regardless of material change	No fixed period No annual renewal requirement: currency of consent assessed contextually, not on a fixed cycle	No fixed period Art. 7(3) requires withdrawal to be as easy as giving consent; consent must remain valid but no fixed renewal period is mandated

3.2.c. The divergences driving this friction are addressed in Section 2, including granular transaction-by-transaction application of BIOC, the omission of a proportionality principle from the Code's drafting, the narrow interpretation of "strictly necessary", the over-reliance on consent, the double-consent architecture, and the destruction right. The Exposure Draft does not substantiate that these divergences are necessary to achieve materially different policy outcomes, particularly given the COPC's intended alignment with the UK AADC. While the Exposure Draft adopts a number of concepts reflected in the AADC, it often operationalises

[27] Australia, *Parliamentary Debates*, House of Representatives, [Second Reading Speech, Privacy and Other Legislation Amendment Bill 2024], Attorney-General (2024): 'The code will align to the extent possible with similar codes in like-minded countries, such as the United Kingdom' <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F28033%2F0046%22>.

them as prescriptive obligations rather than design principles, creating unintended consequences for privacy, safety and functionality.

3.3 Sections 23, 24 and 33: Transparency

Note, the following analysis applies on the basis that the current Division 2 framework is retained.

3.3a. DIGI supports age-appropriate transparency. However, child-friendly notices necessarily simplify complex data practices. Clarification is needed that simplified summaries, layered notices, and visual explanations will not be treated as misrepresentations under the Privacy Act or Australian Consumer Law, provided they accurately reflect the substance of the service's practices. This is particularly important where services apply the Code universally under Section 8(5), rather than undertake age assurance, which in turn, in DIGI's read, may require notices to be designed for a 10-12 year old audience regardless of the service's actual user base (Sections 24(2), 23(3)(c)).

3.3b. DIGI supports the principle that children should be effectively informed when monitoring or location-sharing features are active, consistent with the Code's BIOC framework and children's autonomy interests. However, the Explanatory Statement's references to specific technical implementations, such as an "illuminated icon" visible at all times, are unduly prescriptive. We recommend an outcomes-based, technology-neutral standard for Section 33 that the child is *effectively informed,* allowing services the flexibility to implement contextually appropriate notice designs rather than mandating a particular interface pattern.

3.4 Section 32: Right to request destruction

3.4.a. This new right to request destruction (Section 32) extends beyond existing APP 11.2-11.3 obligations, which instead permit de-identification of personal information. DIGI supports meaningful deletion rights for children, however, section 32 should permit *destruction* or *de-identification*. This would align more closely with the existing Privacy Act framework and broader privacy reforms, while preserving legitimate safety, security and analytical functions where information has already been de-identified or aggregated. For example, de-identified data may be used to detect coordinated harmful behaviour, improve spam and fraud systems, or support service improvements, whereas mandatory destruction in all circumstances may unnecessarily limit these activities despite the privacy risk having been materially reduced.

3.4.b. Permitting de-identification as an alternative outcome would continue to deliver strong privacy protections for children while promoting consistency across Australia's privacy framework and reforms. DIGI also notes that certain categories of data underpinning platform integrity, child safety monitoring, and harm-detection systems may have operational retention requirements that should be expressly acknowledged in the destruction framework, to ensure the Code does not inadvertently undermine the very safety systems it depends on to protect children.

3.4.c. DIGI further recommends that Section 32 be aligned with parental access and correction rights. As currently drafted, the framework grants parents a right to request destruction without providing equivalent rights for children under 15 to access or correct underlying personal information.

3.5 Section 39: Privacy Impact Assessment register

3.5.a. DIGI supports PIA obligations and associated regulatory oversight. However, a public PIA register risks exposing sensitive product, safety, and security information without a commensurate child-privacy benefit. DIGI's view is that OAIC oversight can be achieved through an internal register and mandating on-request production of the register and relevant PIA; we recommend this approach.

3.6 Implementation timeline

3.6.a. DIGI recommends a phased implementation period of at least 12–24 months from registration, with obligations under the Code commencing after the OAIC has published final guidance on key implementation issues, including any age assurance and parental verification required. While DIGI has raised substantive concerns elsewhere in this submission regarding the operability and proportionality of several obligations, implementation of any final requirements will nonetheless require significant changes to product design, governance, data architecture and user-facing systems, together with adequate time for testing and deployment. In particular, services cannot safely design compliant consent and verification flows until there is greater clarity regarding the technical standards and infrastructure required to support them.

3.6.b. A 12–24 month implementation period would be broadly consistent with comparable international frameworks, including the UK AADC and EU GDPR, and would provide industry with sufficient time to implement the Code alongside other major regulatory reforms, including the SMMA, OSA Phase 2 ARM Codes, UTP reforms, and classification and gambling advertising reforms.

Summary of recommendations in Section 3

N. Division 2 consent framework:
   a. Replace the current consent-heavy framework with a more proportionate approach aligned with Australian privacy law and the UK AADC, recognising multiple legal bases for data processing and that meaningful child privacy protection need not depend solely on repeated consent transactions.
   b. Clarify how the Code's consent framework will operate for global services already built around existing consent models, including the UK cookie-consent model to reduce avoidable user experience friction.
   c. If retained in the Code, clarify permissible methods for verifying parental/carer relationship under section 8(3), calibrated to the risk profile of the service and avoiding unnecessary collection of intrusive personal information.
   d. If the two step parent/carer and child consent process is retained, replace "assent" with age-appropriate notice.

O. Section 29 — direct marketing:
   a. Clarify that communications about a service's own features, functionality, user settings, safety tools, account information and product updates are not direct marketing for the purposes of Division 2.
   b. Clarify that "direct marketing" under section 29 does not extend to targeted advertising.
   c. To the extent the Code restricts targeted advertising to children, ensure those restrictions are calibrated consistently with analogous Australian regulatory

frameworks, including broadcasting advertising restrictions, to support regulatory coherence and avoid inconsistent obligations across sectors.

P. Sections 23, 24 and 33 — transparency:

    a. Clarify that simplified, age-appropriate summaries, layered notices and visual explanations will not be treated as misrepresentations under the Privacy Act or Australian Consumer Law, provided they accurately reflect the substance of the service's data practices. This is particularly important where a service applies the Code to all users under section 8(5).

Q. Section 32 — right to destruction: Recast the right as a right to destruction or de-identification at the service's option, consistent with APP 11.2–11.3 and comparable international frameworks, while preserving legitimate safety, security, integrity and analytical functions where privacy risk has been materially reduced.

R. Section 33 — monitoring and geolocation transparency: Adopt an outcomes-based and technology-neutral approach. Guidance should avoid mandating specific mechanisms, such as particular icon types or persistent on-screen indicators, and instead require that children are effectively informed in a contextually appropriate way.

S. Section 39 — PIA register: Amend section 39 so entities maintain an internal PIA register and provide it, and relevant PIAs, to the OAIC on request, rather than publishing the register publicly to remove security risk and competitive sensitivity without reducing regulatory oversight.

T. Implementation: Provide a phased implementation period of at least 12–24 months from registration, with key obligations commencing after final OAIC guidance is issued on foundational obligations and implementation-critical issues, including age assurance.

Appendix

Appendix A: Case studies

The five scenarios below illustrate how users will experience the consent framework under the draft COPC for:

(1) A website with a newsletter on mining stocks, "likely to be accessed" by under 18s (U18)
(2) A 16 year old's personalisation disrupted in an SMMA-covered social media service
(3) A 14 year old using a general-audience marketplace to look for a rugby jersey
(4) A messaging platform regulated under OSA Phase 2 ARM Codes that proactively detects self-harm risks to children
(5) A Multi-child and multi-app household

The following scenarios apply the consent (age 15) provisions and take the Exposure Draft at face value to illustrate its practical consequences. They demonstrate how the Exposure Draft may drive services towards either broader age assurance and parental verification, or child-oriented consent architecture applied across entire services. Both pathways risk increased data collection, consent fatigue, reduced functionality and tension with existing safety systems, without clearly delivering proportionately improved outcomes for children.

DIGI's recommendations, including a more proportionate approach to scope and consent, BIOC as an overarching design principle, and a BIOC-informed interpretation of "reasonably necessary", are intended to address these outcomes while preserving the Code's child-protective objectives.

Scenario 1: A website's newsletter on mining stocks, Section 7 "likely to be accessed" by U18s

Broad reach of scope - mining stocks newsletter

Key issue: Incidental child access should not, by itself, bring an adult-directed service within scope.

Scenario: An ASX mining company has a website, targeted at investors and professionals. It offers an email newsletter that has 1% of under-18 subscribers. It has no child-directed features and does not permit child accounts.

Key friction points:

- The current 'likely to be accessed' threshold would bring this service within scope purely on the basis of incidental access.
- The conservative compliance pathway (age-assure all users) requires collecting age and identity data from a subscriber base of adults, with minimal if any privacy benefit for children where APPs continue to apply.
- In DIGI's reading, the alternative pathway (apply Code to all users) requires adult subscribers to provide consent in a manner that is designed for a 10–12 year old audience.

Outcome under current draft: Neither pathway is proportionate to the risk or the service's profile. A contextual framework for assessing whether children meaningfully access the service, consistent with other privacy frameworks, would make this more workable. Substantive protection for incidental children would apply under current privacy frameworks (including the APPs).

Detailed friction and consequence illustration:

User/service context	COPC requirement triggered	Practical consequence

Adult-focused ASX mining stocks newsletter with no child-directed features	Service may be treated as "likely to be accessed by children" due to low likelihood of under-18 access	A service with minimal child-specific risk is pulled into the Code
Service chooses age-assurance pathway	Age or identity information would need to be collected from adult subscribers	Increased personal information collection with unclear child-centred benefit
Service chooses Code-to-all pathway	Child-oriented notices and settings may apply across the whole user base	Adult users receive experiences designed for children
Service has no meaningful child user base	No clear material harm being addressed	Compliance options and data collection are disproportionate to risk

Scenario 2: A 16 year old's personalisation disrupted in an SMMA-covered social media service

Safety personalisation disrupted in an SMMA-covered social media service

Key issue: Personalisation plays a wide range of roles in most online services. Some personalisation is safety-focused or necessary to provide age-appropriate experiences.

Scenario: A 16-year-old uses a social media service that is subject to the SMMA framework. The service has taken reasonable steps to prevent under-16 users from registering. The service uses behavioural and contextual signals to provide safety-focused personalisation, including reducing repeated exposure to potentially harmful content, limiting unwanted contact from strangers, surfacing wellbeing resources, minimising themes the user selected to view less, and tailoring recommendations to the user's age and maturity.

Key friction points:

- The service may elect to apply the Code to all users under section 8(5), rather than undertake additional age assurance and data collection for all users.
- Under the current drafting, consent would be required before behavioural signals and personalised safety features can operate.
- If consent or opt-in is delayed, unavailable, or withdrawn, the service may need to rely on generic safety settings rather than contextual, age-appropriate interventions.
- These consent processes need to be repeated annually, including for safety-enhancing features used in ordinary social interaction, system recommendations, direct messaging and behavioural moderation.
- The result is that safety-focused personalisation is delayed or degraded for 16 to 17-year-olds who are lawfully permitted to use the service, in tension with obligations under the OSA ARM Codes.

Outcome under current draft: Safety-relevant and age appropriate personalisation may be unavailable, delayed or degraded unless consent requirements are satisfied. A framework intended to protect young people may therefore reduce the ability of services to provide contextual, age-appropriate safety interventions.

Detailed friction and consequence illustration:

User/service context	COPC requirement triggered	Practical consequence
16-year-old lawfully uses an SMMA-covered social media service	Service may apply the Code to all users under s 8(5) rather than undertake further granular age assurance	Child-oriented consent architecture applies broadly
Service uses behavioural and contextual signals for safety personalisation	Consent or opt-in control would be required before those signals can be used	Safety-focused features may be delayed
User engages with recommendations, chat or direct messaging	Consent or opt-in control is needed for system recommendations, behavioural moderation and safety signals	Generic safety settings may replace contextual, age-appropriate interventions
Consent is delayed, unavailable or withdrawn	Personalised safety systems cannot fully operate	Reduced ability to limit harmful content, unwanted contact, or self-harm risks
Annual renewal applies	Consent workflows repeat each year until the user turns 18	Ongoing disruption to ordinary use and safety functionality

Scenario 3: 14-year-old using marketplace to find a rugby jersey

Safety and personalisation restrictions on a general-audience marketplace

Key issue: Personalisation can support relevance, fraud prevention, and safer marketplace or e-commerce experiences. Restricting it reduces safety and utility.

Scenario: A large general-audience marketplace has terms of service prohibiting under-18 accounts and actively works to prevent child registration. It has some incidental child users. A 14-year-old uses the platform to find a rugby jersey. The service uses personalisation and behavioural signals to improve search relevance, identify suspicious sellers, suppress scam listings, and highlight age-appropriate products and minimise any inappropriate ad targeting such as for alcohol or other adult only products.

Key friction points:

- The Code would trigger verified parental consent plus child assent before ordinary browsing, personalised search results, saved preferences and fraud-prevention features can operate.
- A parent or carer would need to verify identity and complete a consent workflow before the child can proceed.
- Personalised search and recommendations are unavailable or delayed, meaning the child sees generic results rather than items matching their size, team, and prior search context.
- Safety-related personalisation, including suspicious seller detection, scam suppression and age-appropriate recommendations, are also restricted despite reducing risk to the user.

- Ads are not properly calibrated and send targeted beer-themed content.
- Subsequent features such as wish lists, price alerts and saved carts likely require their own consent transactions, with positive renewal from both parent/carer and child required again after 12 months.

Outcome under current draft: Routine shopping activity becomes subject to parental verification and repeated consent processes. At the same time, safety-focused personalisation designed to identify scams, fraudulent sellers, and relevant products are unavailable or delayed until consent requirements are satisfied, reducing functionality without a clear corresponding privacy benefit.

Detailed friction and consequence illustration:

User/service context	COPC requirement triggered	Practical consequence
14-year-old incidentally uses a general-audience marketplace to find a rugby jersey	Verified parental consent and child assent may be required before ordinary browsing and personalised search operate	Routine shopping becomes subject to repeated parental verification
Marketplace uses search history, size, team preferences and context	Personalised search would be treated as requiring consent	Child sees generic results rather than relevant items
Marketplace uses behavioural signals to suppress scams or suspicious sellers	Safety-related personalisation would also be delayed or restricted	Reduced scam and fraud protection
Child tries to save item, use wish list or receive price alerts	Separate consent may be required for each feature	Repeated consent transactions for ordinary marketplace functionality
Annual renewal applies	Parent/carer and child must renew consent after 12 months	Friction repeats without proportionate privacy benefit

Scenario 4: Messaging platform that proactively detects self-harm risks to children

The safety tension on a teen messaging platform

Key issue: The Code should expressly recognise, at a minimum, safety-related processing required by other Commonwealth laws as permitted or "reasonably necessary".

Scenario: A teen messaging platform is regulated under OSA Phase 2 ARM Codes, which - to the extent technically feasible - require it to proactively detect at-risk child behaviour. It uses engagement patterns and content signals to surface crisis resources for children showing signs of self-harm.

Key friction points:

- Section 9(1) requires that only data 'strictly necessary' to provide the service is collected by default.
- The OAIC's Explanatory Statement indicates personalised recommendations and behavioural analysis would not generally be 'strictly necessary.'
- To detect self-harm risk, the platform must - to the extent technically feasible - analyse message content and engagement patterns, processing the child's sensitive personal communications.
- This is exactly what OSA ARM Code compliance requires. But under a strict reading of Section 9, it is not 'strictly necessary' to provide a messaging service.

Outcome under current draft: The platform faces an unresolved legal tension: comply with the COPC and disable the safety system that the OSA requires; or comply with the OSA and breach the COPC. At-risk children lose protection at the moment they need it most. This conflict must be resolved before the Code is registered.

Detailed friction and consequence illustration:

User/service context	COPC requirement triggered	Practical consequence
Teen messaging platform is regulated under OSA Phase 2 ARM Codes	Platform is expected to detect and respond to at-risk child behaviour	Safety systems need to analyse engagement and content signals
Platform uses signals to identify self-harm risk and surface crisis resources	Section 9 "strictly necessary" default may restrict behavioural analysis	Safety processing may not clearly fit within "strictly necessary" to provide messaging
Platform complies strictly with COPC	Safety detection system may need to be limited or disabled	At-risk children may lose protection
Platform complies with OSA safety obligations	Same processing risks being inconsistent with COPC	Legal and operational tension between safety and privacy obligations
Child shows signs of acute distress	System cannot confidently act without regulatory clarity	Intervention may be delayed at the moment it is most needed

Scenario 5: Multi-child and multi-app household: implications of the current consent framework

Consent fatigue in a family with two children

Key issue: More consent does not necessarily produce more meaningful consent. Repeated consent and verification requirements may undermine the very objective they are intended to achieve.

Scenario: A parent has two children aged 12 and 14 who each use a minimum five COPC-regulated services: social media, gaming, an education app, music streaming, and video.

Key friction points:

- At sign-up: verified parental consent transaction plus separate child assent for each service (10 consent transactions across 5 services and 2 children).
- Annually: the entire process must be repeated for each service, on each service's own renewal cycle, producing up to 10 annual re-consent obligations at unpredictable times through the year.
- Per feature: separate consent required for each material data use (safety signals, social and service recommendations, chat moderation), multiplying the transaction count further.
- Each consent transaction requires the parent's identity to be verified, potentially requiring personal information to be shared.

Outcome under current draft: Numerous consent transactions are required in one household for multiple service use (e.g. a minimum 20 annually for 5 services, assuming no additional features requiring additional data use is sought). Annual re-consent requirements risk creating consent fatigue across multiple services, resulting in users routinely clicking through requests rather than making informed decisions. In settings where there is limited practical ability to refuse consent, such as education, the framework may further undermine the objective of meaningful consent.