Tech Council of Australia

# Children's Online Privacy Code

Tech Council of Australia submission

June2026

# 1. Introduction

Thank you for the opportunity to make a submission regarding the Children's Online Privacy Code exposure draft. The Tech Council of Australia (TCA) believes in the importance of improved privacy protection, especially for children.

The TCA is Australia's peak industry body for the tech sector. The tech sector is a key pillar of the Australian economy, with the tech sector Australia's third largest industry behind mining and banking, and Australia's seventh largest employing sector. The TCA represents a diverse cross-section of Australia's tech sector, including startups, scale-ups, venture capital funds and global tech companies, many of whom provide services directly to consumers and small businesses.

TCA supports the objective of protecting children's privacy online and welcomes the OAIC's intention to align the Code with the United Kingdom's Age Appropriate Design Code (AADC). This submission makes ten recommendations to ensure the Code is workable, proportionate to actual privacy risk, technically feasible, and coherent with parallel reforms, including reforms to the Online Safety Act and in relation to unfair trading practices. Our central concerns are:

- **Scope and proportionality (s 5)** — the "likely to be accessed by children" threshold is broad and undefined, and conflates a child's exposure to an online service with increased risk or harm. The Code does not distinguish between general purpose online services likely to be accessed by children and services specifically designed for children, without regard to the materially different risk profiles across platforms.The Code could adopt a "directed to children" standard that is consistent with US COPPA, which is applied to services whose design, content, or marketing is oriented towards a child audience. At a high level, a risk-tiered framework, proportionate to potential harm, should apply to both scoping and compliance obligations.
- **Exclusions (s 6)** — currently, the Code only expressly excludes carriage service providers, and does not recognise the extremely broad-range of services that fall within the scope of a designated internet service (DIS). Enterprise DIS, as defined under the Online Safety Act's codes and standards, should be excluded from this Code, as they would not meet the "likely to be accessed by children" threshold and should not be required to make this assessment.
- **The "strictly necessary" standard (s 9)** – the standard creates significant uncertainty for legitimate trust, safety and security uses of data, and should be reframed as "reasonably necessary" with specific permitted purposes or, alternatively, supported by binding guidance.
- **Consent architecture** — the 12-month consent refresh, prescriptive parental consent and active "assent" requirements risk consent fatigue, user drop-off, and worse outcomes for children than a more measured approach. This is further complicated by use cases where the parent consents on behalf of the child against the child's wishes or vice versa.

- **Right of erasure (s 32)** — the Code goes beyond APP 11 and the broader Privacy Act reform process by treating de-identification as insufficient. Targeted exceptions are needed for technical feasibility, cyber security and fraud, and regulatory record-keeping.
- **Public register of PIAs (s 39)** — publishing a register raises commercial sensitivity and cyber security risks, is out of step with international practice and should be removed.
- **Implementation timeframe** — the Code requires significant re-architecting of digital services and supporting technologies that are not yet mature. A minimum 24-month transition is necessary, accompanied by detailed OAIC guidance that is co-designed with industry, consistent with international best practice.

**Consolidated recommendations**

**Recommendation 1:** Before commencement, publish binding guidance on the scoping test — particularly the "attractive to children" limb — with worked examples. Introduce a preliminary step that carves out services presenting low or negligible child privacy risk from the Code's substantive obligations. Apply a tiered risk framework, modelled on the Online Safety Act codes, across both scoping and compliance obligations.

**Recommendation 2:** Enterprise DIS, as defined under the Online Safety Act's codes and standards, should be excluded from this Code, as they would not meet the "likely to be accessed by children" threshold and should not be required to make this assessment. Consistent with the approach taken by the eSafety Commissioner, obligations should be proportionate to the actual risks posed by services.

**Recommendation 3:** Replace "strictly necessary" with "reasonably necessary," in alignment with the existing Australian Privacy Principles, supported by an enumerated, non-exhaustive list of permitted purposes that includes trust and safety, fraud and cyber security, content moderation, product improvement and machine learning used for those purposes that can be in the "best interest" of a child.

**Recommendation 4:** Replace the mandatory 12-month refresh with a requirement to send periodic, age-appropriate privacy reminders at annual intervals that highlight current settings and how to withdraw consent.

**Recommendation 5:** Amend section 20 so that assent for young children operates as an age-appropriate notice requirement, with active assent reserved for older children closer to the age of consent. Clarify the relationship between sections 20 and 13 to avoid overlap.

**Recommendation 6:** Align section 32 with APP 11 and the Privacy Act reform process. Permit de-identification and the concept of putting data "beyond use" as a compliance route where destruction is not technically feasible. Add explicit exceptions for cyber security and fraud prevention, AML/CTF and other regulated record-keeping obligations, and data needed to demonstrate compliance to regulators. Address the interaction with other binding codes (including SPF codes) through an explicit conflict-of-laws provision.

**Recommendation 7:** Remove the public register requirement. Retain the OAIC's ability to request PIAs on a confidential basis. If a transparency mechanism is desired, permit publication of a

brief, high-level summary after a feature has been released, and exempt unreleased products and detailed control information.

**Recommendation 8:** Codify in the Code the Explanatory Statement's language on commercial interests, and provide worked examples to support consistent interpretation.

**Recommendation 9:** Amend the Code (or the Explanatory Statement) to carve out enterprise services from the Code. For educational services in which the customer administers data settings, attach the Code's substantive obligations (such as consent, erasure and PIA requirements) to the customer rather than the underlying service provider.

**Recommendation 10:** Set commencement to a minimum of 24 months after the Code is made, aligned to the commencement and review milestones of Part 4A of the Online Safety Act and other intersecting reforms.

## 2. Scope and proportionality

**Section 7** applies the Code to social media, relevant electronic and designated internet services (DIS) that are "likely to be accessed by children" or "primarily concerned with the activities of children." The threshold is imported from section 26GC of the Privacy Act, but is not defined in the Code and the Explanatory Statement does not provide a substantive interpretation. This generates uncertainty for services that are visually appealing but neither target children nor have a significant child user base.

The categories of services subject to the Code are imported from definitions contained in the Online Safety Act's DIS standard and code is extremely broad, and includes websites, apps and streaming services. Specifically, the DIS Standard includes definitions such as "enterprise DIS" (examples include websites for ordering commercial supplies by enterprise customers, and services providing pre-trained AI or machine learning models for integration into a service deployed by an enterprise customer) , "classified DIS" (such as films and video games that are or would be classified), "general purpose DIS" (websites primarily providing information for business, news, educational, government or other specified purposes). There is no recognition of these different categories of DIS services in the Code, nor is there consideration of the privacy risks these different categories of service pose for children.

The Code also conflates two distinct concepts: services likely to be accessed by children, and services likely to cause privacy harm to children. Services that meet the "likely to be accessed by children" threshold should, as a subsequent additional step, also demonstrate the level of privacy risk for children. Services with a high privacy risk should be subject to the most obligations under the Code. Without this additional step, every website "likely to be accessed by children" would be required to ascertain the age of every end-user before the end-user could access the website. The data minimisation principle the OAIC has promoted is not advanced by requiring age assurance steps where the underlying privacy risk is negligible.

**Section 8(2)** contemplates a risk-based approach for age assurance, and paragraph 6 of the Explanatory Statement confirms this is the intention. TCA supports this approach but considers

it should be extended across the Code. As drafted, the proportionality concept does not reach section 9 (strictly necessary), section 13 (parental consent), section 20 (assent), or section 32 (destruction). The proposed legislated digital duty of care under the Online Safety Act is intended to apply a risk-based framework, where obligations are proportionate to the level of risk of a service.

*Comparison to UK*

Although the Draft Code draws from the UK Age Appropriate Design Code (AADC)'s risk-based approach to age assurance, it diverges in that its current drafting would not allow for low risk services to forgo age assurance altogether.

Under the UK framework, the level of age assurance required scales to the risk profile of the service. The ICO is explicit that entities have flexibility to determine how to apply the standard based on the risks arising from their specific data processing activities, and is deliberately non-prescriptive about methods or certainty thresholds.The Draft Code does not offer equivalent flexibility. While a low-risk service may reduce the level of assurance required, the obligation to conduct age assurance does not appear to be removed altogether. This means, as written, even services that pose minimal privacy risk to children must still clear an age assurance threshold of some kind before collecting data.

The Code should have a more explicit risk-based approach and provide a framework of factors that would indicate whether a service a) is likely to be accessed by children, and b) differentiate between services that have a higher privacy risk for children and those that are a lower privacy risk.

Businesses should be assisted in assessing whether a child is likely to access the service. The test for this could include whether:

- Accounts are created through adult-associated payment methods
- Youth experiences are managed through an adult account (for example, the child profile or part of the service that is available to children should be the only one in scope of the Code)
- A service actively removes known child users
- A significant number of children use that service
- The service contains design features that would encourage or attract children, or
- If the service includes ads targeting children.

An assessment of risk of a service should also be captured by the Code, including for example whether a service:

- Has features that would enable contact between a child and a stranger
- Predominantly contains user-generated content
- Has child profiles or experiences that would reduce the risk of privacy harms arising to children.

**Recommendation 1:** Before commencement, publish binding guidance on the scoping test — particularly the “attractive to children” limb — with non-exhaustive examples. Introduce a preliminary step in the Code that carves out services presenting low or negligible child privacy risk from the Code’s substantive obligations. Apply a tiered risk framework, modelled on the Online Safety Act codes, across both scoping and compliance obligations.

**Recommendation 2:** Enterprise DIS, as defined under the Online Safety Act’s codes and standards, should be excluded from this Code, as they would not meet the "likely to be accessed by children" threshold and should not be required to make this assessment. Consistent with the approach taken by the eSafety Commissioner, obligations should be proportionate to the actual risks posed by services.

## 3. The “strictly necessary” standard (section 9)

The "strictly necessary" threshold for collection of personal information is highly onerous and risks undermining a range of activities that are genuinely protective of children — including trust and safety functions, fraud prevention, cybersecurity, content moderation, accessibility improvements and privacy protective product development. These may not always be “strictly necessary” to provide the service in the narrowest sense, but can be beneficial and protective for children.

Section 9(1) requires, by default, that an entity only collects, uses or discloses personal information about a child that is “strictly necessary” to provide its service. Paragraph 9 of the Explanatory Statement describes this as “essential,” a “narrower and more protective threshold than reasonably necessary.”

This threshold creates substantial uncertainty for activities that benefit children themselves — including content moderation, fraud detection, training and tuning of trust and safety models, anti-abuse measures and accessibility improvements. These activities are not “essential” to providing the service in a narrow sense but are clearly in users’ interests. Without guidance, Australian businesses face cost in legal review, conservative compliance choices that disadvantage children, and inconsistency between providers.

In addition, we are concerned that the "strictly necessary" test is intended to limit a service’s ability to personalise content. For content service providers, such as streaming services, personalisation of content is a core value proposition and expectation of end-users, and without this, significantly degrades the service. Content recommendations based on viewing or listening history could be considered as not "strictly necessary". This is a disproportionate outcome, with unclear privacy benefits for end-users who are children.

If the strictly necessary threshold is retained, there should be clear permitted purposes as exceptions to the strictly necessary threshold, with a catch all default, such as “or where in the public interest, or the interest of the child or children more generally”.

**Recommendation 2:** Replace “strictly necessary” with “reasonably necessary,” supported by an enumerated, non-exhaustive list of permitted purposes that includes trust and safety, fraud and cyber security, content moderation, and machine learning used for those purposes.

# 4. Consent architecture (sections 13–20)

Whilst we recognise and support the broader policy intent behind improving children's understanding of how their personal data may be used online, and increasing their agency over this, we believe the proposed architecture of consent is highly onerous, technically complex and is not commensurately improving a child's safety online.

## 12-month consent refresh

Section 15(4)(b) caps consent at 12 months. With a broad application of in-scope services, frequent re-consent prompts risk consent fatigue, user drop-off, may undermine children’s access to age-appropriate services they currently use safely and ultimately not improve children’s agency in practice. They may normalise click-through behaviour, increase the decision-making burden on children and parents, and interrupt access to beneficial services. For example, online educational platforms used for children's ability to complete school work risks disruption to carrying out curriculum if consent is required at the child level and needs annual renewal.  The requirement is also out of step with the consent framework being implemented under Part 4A of the Online Safety Act and reforms to unfair trading practices, which together push users towards account creation rather than guest interactions.

**Recommendation 3:** Replace the mandatory 12-month refresh with a requirement to send periodic, age-appropriate privacy reminders at annual intervals that highlight current settings and how to withdraw consent.

## Parental consent (section 13)

Section 13 requires entities to obtain consent from a person with parental responsibility for children under 15, and to take reasonable steps to confirm that person’s status. Three issues arise. First, the technology to verify parental responsibility is not yet mature; older siblings or other adults may pose as parents. There are also significant barriers to an APP entity being able to confirm whether someone has actual parental or guardianship for a child. For example, if they were required to provide a birth certificate and the ID documents of the parent, then this would be inconsistent with the data minimisation principle.

Second, the work underway on age assurance providers under the Online Safety Act has highlighted the need for accreditation and testing of providers; the same should apply to parental consent providers. Third, in sensitive scenarios (for example, a child seeking online help in relation to a family situation) obtaining parental consent is impractical or unsafe.

We do not oppose parental or guardian involvement in consent frameworks where it is appropriate and operable. For educational platforms, teacher or school-mediated consent aligns with the US COPPA model and represents a workable framework for lower-risk platforms. The

Draft Code would benefit from adopting a similarly differentiated model which recognises that a blanket parental consent requirement across all service types is neither practical nor safe in every context.

**Recommendation 4:** Coordinate with the eSafety Commissioner to establish a testing and accreditation pathway for parental consent providers. Recognise account-level parental controls, teacher or school-mediated (for example, where a parent has set up a supervised child profile) as constituting parental consent for the purposes of section 13. Expand the section 13(4) exception to permit anonymous access to safety-relevant information and support services, drawing on the UK ICO's position on "special cases."

## 5. Right of erasure and de-identification (section 32)

Section 32 requires destruction of personal information on request, subject to limited exceptions, and paragraph 21 of the Explanatory Statement provides that "de-identification of personal information will not be sufficient." This goes beyond APP 11.2 and the broader Privacy Act reform process, in which the role of de-identification remains under consideration. The OAIC's existing "beyond use" guidance acknowledges circumstances in which technical destruction is not feasible.

Four further issues arise. AML/CTF obligations and emerging Scams Prevention Framework codes impose multi-year retention obligations. Regulators routinely require retention of data during investigations to verify a respondent's compliance, which conflicts with strict destruction obligations. And retention of certain data is essential to cyber security and fraud prevention, including information sharing between regulated entities.

In addition to these issues, destruction of information may not always be technically feasible. For example, for cloud service providers, complete destruction may not be technically feasible given distributed architectures involve data replicated across backups, disaster recovery systems, and operational logs designed for resilience and redundancy.

The technical feasibility of this obligation is further complicated when a child, or parent on behalf of a child, has consented to the child's personal information or data to be used to train AI models. Once consent has been provided and the data has been used to train the model, it can no longer be feasibly extracted from the model and destroyed.

**Recommendation 5:** Align section 32 with APP 11 and the Privacy Act reform process. Permit de-identification as a compliance route where destruction is not reasonably practicable. Add explicit exceptions for cyber security and fraud prevention, AML/CTF and other regulated record-keeping obligations, and data needed to demonstrate compliance to regulators. Address the interaction with other binding codes (including SPF codes) through an explicit conflict-of-laws provision.

## 6. Public register of Privacy Impact Assessments (section 39)

**Whilst we agree that privacy impact assessments should be completed for features or products that may have an impact on children, the requirement for them to be posted on a public register unhelpfully conflates transparency with disclosure.**

We recognise the public register requirement reflects transparency principles applicable to government agencies, however private entities operate under very different constraints with commercially sensitive product roadmaps, needing to protect intellectual property, and security architecture which is not analogous to public sector information.

Section 39(1)–(3) requires entities to maintain and publish a register of PIAs online. This raises three concerns. First, detailed control information surfaced in PIAs can be exploited by malicious actors - particularly controls relating to privacy, trust and safety, child safety, abuse prevention and security, where public disclosure risks making those controls easier to circumvent. Second, publishing details, including for unreleased products, risks revealing commercially sensitive roadmaps and intellectual property. Third, the administrative burden of maintaining a public register at scale is substantial and out of step with the UK AADC, which does not require public publication.

**Recommendation 7:** Remove the public register requirement. Retain the OAIC's ability to request PIAs on a confidential basis. If a transparency mechanism is desired, permit publication of a brief, high-level summary after a feature has been released, and exempt unreleased products and detailed control information.

## 7. Best interests of the child

Sections 10, 11, 38 and 40 require handling of children's personal information to be consistent with the best interests of the child. TCA supports this principle. Paragraph 10 of the Explanatory Statement helpfully states that "an entity's commercial interests may not be incompatible with the best interests of the child." This language, drawn from the UK ICO's guidance, should be reflected in the Code itself with worked examples — for instance, free services funded by responsible, age-appropriate advertising or personalisation.

**Recommendation 8:** Codify in the Code the Explanatory Statement's language on commercial interests, and provide worked examples to support consistent interpretation.

## 8. Enterprise and educational services

The Code does not distinguish between consumer-facing services and enterprise or educational services. Consistent with the commentary above, enterprise services should not be caught by the Code due to the low privacy risk associated with these services (and the unlikelihood of them being accessed by children). In educational contexts the customer (a school, employer or other organisation) typically administers settings relating to data retention, disclosure and

destruction. Providers can retain control over platform level settings, security and subprocessor relationships, but should not bear responsibility for deployment choices made by the customer that may be customised to their own working environment, where the provider's direct control is minimal. Imposing identical obligations creates compliance risk for activities the provider cannot effectively control. Other Australian regimes — including the Online Safety Act codes — recognise this distinction through tiered obligations.

**Recommendation 9:** Amend the Code (or the Explanatory Statement) to carve out enterprise services from the Code. For educational services in which the customer administers data settings, attach the Code's substantive obligations (such as consent, erasure and PIA requirements) to the customer rather than the underlying service provider.

## 9. Implementation timeframe

Section 2 is currently "[to be drafted]." A minimum 24-month transition is required. The Code will demand significant re-architecting of services for tech companies, reworking consent flows, introducing age assurance, changing data retention and destruction processes, updating internal training and PIAs, and this will also affect many businesses that have not yet recognised they are within scope (given the broad scope of the Code). Several supporting technologies, including parental consent and age assurance providers, are not yet mature and require their own accreditation processes.

**Recommendation 10:** Set commencement to a minimum of 24 months after the Code is made, aligned to the commencement and review milestones of Part 4A of the Online Safety Act and other intersecting reforms.