Submission to

SUBMISSION TO THE OAIC
DRAFT CHILDREN'S ONLINE PRIVACY CODE

on behalf of

Australian Association of National Advertisers

June 2026

Introduction

The Australian Association of National Advertisers (AANA) welcomes the opportunity to provide this submission to the OAIC on the Draft Children's Online Privacy Code. As the peak body representing Australia's advertising and marketing ecosystem, the AANA is fully committed to protecting children's digital safety and privacy online.

This submission aims to flag issues around operational feasibility, regulatory overlap, and unintended consequences that are likely to may flow from the Code's current drafting.

Summary

The submission highlights five primary areas of concern:

- **Disproportionate Age Assurance Requirements:** The draft COPC departs from the UK AADC by requiring services to verify users against specific age boundaries. This forces platforms to ascertain the ages of adults, which is disproportionate, burdensome, and goes against the UK AADC framework.
- **Regulatory Alignment:** The COPC, as currently drafted, deviates from established Australian privacy law as well as the UK AADC, as was the mandate to OAIC. Additionally, the Code is being developed concurrently but separately from broader Tranche 2 privacy reforms, risking immediate regulatory misalignment.
- **Timelines:** Additionally, complex backend IT overhauls cannot be completed by 10 December 2026. IT system and compliance work normally commences once there is regulatory certainty, upon the passing of legislation or the registration of a Code. AANA believes that an extended implementation window of at least 18-24 months is required to allow businesses to appropriately re-engineer data systems.
- **Scope Creep & The "DIS" Dilemma:** Broadly defining "Designated Internet Services" (DIS) drags standard commercial platforms, brands, and retailers into scope simply because they may meet the "likely to be accessed by children" threshold. This creates compliance deadlocks for everyday interactions like connected vending machines, retail kiosks, loyalty schemes, and streaming apps, which cannot practically verify age.
- **The Identity & Verification Paradox:** The Code requires all DIS, RES and SMS services that meet the "likely accessed" threshold to ascertain the age of all end users before they collect personal information and to identify parents of children in certain circumstances, leading to increased data capture. This actively conflicts with APP 2 (Anonymity and Pseudonymity). However, Division 5 of the Code then creates a compliance loop by requiring immediate destruction of verification data. This will leave businesses without a defensible audit trail to prove to the OAIC that they verified a user's authority before deleting or releasing information and also unable to provide age-appropriate experiences by ensuring children do not see inappropriate ads or other content.
- **Digital Exclusion & Marketing Ambiguity:** Setting the digital age of consent at 15 and requiring "Double Assent" (parental intervention) risks cutting off teenagers from vital online services and employment tools. Furthermore, the definition of "direct marketing" remains vague. Clear safe harbours defining acceptable age verification methods, confirmation that first-party content

recommendations do not constitute direct marketing, and a technical correction to a drafting typo in Section 20(6).

Strategic and Structural Concerns

Inconsistencies with UK's AADC

The draft COPC departs from the UK AADC in a number of significant respects, without justification or evidence, with concerning implications. For example, it requires entities to determine a user's age against both the 15 and 18 age boundaries, rather than an age range such as 18+ as in the UK AADC. One implication of this is that services must even ascertain an adult end-user's age. This is disproportionate and contrary to the UK AADC, which requires instead that online services understand the "age range of children likely to access the service" (i.e. 18+ is sufficient).

Consistency with Established Australian privacy law

The COPC should not introduce any measures that contradict the current Privacy Act or anticipated tranche 2 reforms. The COPC and Tranche 2 privacy reforms should be structurally coordinated.

The draft COPC deviates from established privacy law in a number of ways. For example, it introduces a "strictly necessary" standard that is new in Australian privacy law and has no legal meaning. This new requirement could inadvertently prevent beneficial data processing for children, including personalisation (also known as exclusion targeting) to provide age-appropriate content and safety and integrity measures.

Forcing the industry to comply with a standalone Code, only to overhaul it months later to align with new federal Tranche 2 privacy legislation, creates unjustifiable compliance friction. For example, COPC's proposed right to destruction and not permitting de-identification appear to be taking a different approach to how the same issue has been considered in the context of tranche 2 reforms. Also, coordination with the new Automated Decision-Making (ADM) transparency obligations would be optimal.

Implementation Timeline and IT Architecture

The OAIC has sought feedback on appropriate implementation timeframes. Given the current drafting of the Code will capture general audience services like retail self-serve checkouts, extensive work will be required to scope and implement the required IT, policy, processes and training changes. Comprehensive IT architecture overhauls - including data segregation, age-gating mechanisms, and automated deletion workflows - cannot be executed overnight. The AANA requests an extended implementation window of 18-24 months from the date the final Code is registered.

The "Best Interests of the Child" (BIOC) Standard

The introduction of the BIC standard represents a shift from the current framework. Under APP 3, data handling is bound by "commercial necessity" and whether collection is "reasonably necessary" for a business function. The draft Code subordinates commercial necessity to a multi-faceted well-being standard.

While we support safe environments for children, introducing a sweeping duty of care via an industry code—rather than through standard legislative channels—amounts to regulation by stealth. The

OAIC must provide objective, clear legal boundaries on how businesses are to balance commercial utility with the BIC standard.

The OAIC may consider replicating the UK Information Commissioner's Office guidance on the "best interests of the child" test, which provides that commercial interests may not be incompatible:

> *"Taking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests. Your commercial interests may not be incompatible with the best interests of the child, but you need to account for the best interests of the child as a primary consideration where any conflict arises."*

Scope and Coverage Clarity (The DIS Dilemma)

The inclusion of Designated Internet Services (DIS) as defined by reference to the *Online Safety Act 2021* creates vast, ambiguous territory. Because the draft Code captures any service "likely to be accessed by children" or "primarily concerned with the activities of children," ordinary commercial entities are pulled into scope.

To illustrate the technical and operational challenges this poses for the retail, brand, and media sectors, the AANA presents four realistic case studies requiring definitive OAIC guidance:

Case Studies: Operational Vulnerabilities

- **Case Study 1: Connected Vending Machines & Retail Self-Serve Kiosks**

Online-connected vending machines, retail self-serve checkouts and in-store fast-food ordering kiosks theoretically fall under the definition of a DIS. Because physical, fast-transaction interfaces cannot practically execute age verification, they would be legally forced to deploy ultra-high privacy default settings for **all users** (including adults), restricting basic functional data processing.

- **Case Study 2: Beauty Store Loyalty Schemes**

A cosmetics retailer operates a rewards program. If a teenager signs up to receive loyalty discounts, the retailer faces complex identity validation rules. If the retailer uses a simple "year of birth" age gate, it remains unclear whether the OAIC deems this legally sufficient to prove the app is not "likely to be accessed by children" under 15. It is likely that children under 15 will be excluded from accessing and benefiting from retail loyalty schemes once this Code takes effect.

- **Case Study 3: Independent Streaming Services (Non-Broadcast)**

Video-on-demand services operating under a traditional broadcasting license are exempt. However, standalone brand streaming apps, niche sports platforms, or hobbyist video networks fall under the DIS category as a "classified DIS". The Code dictates that they must configure high privacy defaults for all data where age verification cannot be undertaken. Verifying the age of all viewers in a room at any given time is impossible for these platforms. Streaming platforms currently take note of the programs viewed by each user and use that data to provide recommendations as to other programs the user might enjoy. This may come within the definition of direct marketing. It is unclear how this recommendation activity could continue once the Code takes effect if a high privacy default setting is applied to all users.

- **Case Study 4: Online Brand Competitions**

A consumer brand runs an online sweepstakes on its corporate website. To avoid triggering the Code's heavy requirements, the brand must deploy robust age gates to exclude children, unintentionally restricting harmless brand engagement.

Age Assurance, Consent, and Anonymity

Privacy Paradox - Conflict with APP 2 (Anonymity and Pseudonymity)

The draft Code creates an irreconcilable tension with APP 2, which guarantees individuals the option of interacting anonymously or pseudonymously.

Draft Code Requirement		**APP 2 Core Mandate**
Prove Age / Verify Identity	vs.	Right to Interact Anonymously
(Requires MORE Data)		(Requires LESS Data)

To verify that a user is over 15, or to verify that an adult is indeed the "person with parental responsibility" under Section 13, entities will be forced to collect **more** personal information (such as IDs or biometric markers). This creates a privacy paradox where businesses must capture sensitive information purely to comply with a privacy-saving rule.

The Verification Loop and Deletion (Division 5)

Division 5 mandates that sensitive information used for age checks must be destroyed immediately after verification. Furthermore, organisations must verify the identity of a parent requesting data deletion under Division 4 or 5 but are prohibited from retaining the data gathered during that specific verification process.

This creates a circular compliance trap. Companies are forced to validate identity to prevent malicious data deletion or unauthorised access yet cannot retain a defensible audit trail to prove to the OAIC that they verified the applicant's authority in the first place and may compromise the safety and integrity of services.

Social Impacts: The Under-15 Digital Divide

Codifying the digital age of consent at 15 - and requiring a strict "Double Assent" rule (where a child must assent to the platform contacting their parent) - will cut young people out of digital society. For example, a vulnerable 14-year-old seeking casual employment or managing a basic bank account may be unable to secure an abusive or absent parent's digital consent, effectively locking them out of modern economic participation. Also, the technical infeasibility of certain requirements and risks associated with collecting age verification data will mean that companies may opt not to deal with people under the age of 15, meaning children will be unable to participate in society as they are today.

The UNCRC General Comment on the Rights of the Child in the Digital Environment states: "*the best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context*". The BIOC requires balancing privacy with a young person's right to: identity; freedom of

association; freedom of expression (including to seek, receive and impart information); education; and the right to play and take part in a wide range of activities.

Direct Marketing, Personalisation and Transparency

Definition of Direct Marketing

Section 29 introduces a 12-month "hard cap" on consent for non-essential activities, requiring a mandatory reset of marketing permissions every year. The AANA requires urgent clarity on what constitutes "direct marketing" in a modern digital environment.

- **First-Party Personalisation:** If a streaming app recommends a cartoon to a child based entirely on their previous viewing history within the platform, does this trigger Section 29?
- **Operational Communications:** If a child purchases an item or wins a brand competition and opts to receive a functional receipt or prize notification via email, does the inclusion of a brand logo reclassify that transactional communication as direct marketing?

Protecting Children from Inappropriate Content

The advertising regulatory system requires advertisers to ensure that ads for certain products (such as alcohol, gambling or less healthy food) are not shown to children. Personalisation and exclusion targeting is essential for a tailored and safe online environment for children and other vulnerable people. On the other hand, the COPC appears to assume that all use of children's data and personalisation is inherently negative.

The requirement to provide children with access to a service even if they do not consent to the use of their data for purposes the OAIC deems to not be "strictly necessary" (such as personalised content) opens the door to making online experiences less safe for children. A non-personalised experience may make it more likely that teens will come across content and ads that are age-inappropriate, as apps may be prohibited from using algorithms to filter this content from their experiences.

Drafting Typo Note

The AANA notes a technical drafting error in **Section 20(6)**. The text cross-references paragraph *(5)(b)(ii)*, but based on the structural flow of the provision, it should correctly reference paragraph **(5)(b)(iii)**.

Summary of Requests for Guidance

The AANA formally requests that the OAIC include clear, legally binding guidance and practical safe harbors within the final Code text regarding:

1. **Proportionality:** As currently drafted, the "likely to be accessed by children" test could require nearly all retail businesses to undertake age verification. The test should be clarified and the Code should adopt a more proportionate, risk-based approach. Even where a service falls within scope, low-risk services should either be excluded or subject only to limited obligations. The Age Appropriate Design Code provides a more flexible and appropriate model by allowing obligations to be applied in a risk-based and proportionate way.

2. **Acceptable Age Verification:** Clear, tiered definitions of what methods satisfy "reasonable steps" to ascertain age based on risk profiles (e.g. when a birth-year entry is sufficient vs. when high-fidelity assurance is required).
3. **Parental Verification Limits:** A prescriptive, low-friction standard for verifying a "person with parental responsibility" that explicitly protects companies from breaching APP 2 or APP 3.
4. **The Record-Keeping Safe Harbor:** Clear rules allowing entities to retain a minimalist, secure, and hashed audit trail to prove compliance with deletion and access requests without violating Division 5.
5. **Exemptions for Functional Personalisation:** Explicit confirmation that basic first-party content recommendations and standard transactional emails (e.g. digital receipts) do not constitute direct marketing under Section 29.

Further Consultation

The AANA would welcome an opportunity to discuss in more detail with the OAIC the issues in our submission. Please contact [redacted] regarding opportunities for further consultation.