AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

Draft Children's Online Privacy Code

June 2026

The Australian Retail Council (ARC) welcomes the opportunity to provide a submission to the Office of the Australian Information Commissioner (OAIC) about the draft Children's Online Privacy Code (the Code).

ARC represents the Australian retail sector. Valued at $444 billion, retail is the nation's second largest private sector employer, supporting more than 1.5 million jobs, including for more young Australians aged 15 to 24 years than any other industry.

Our membership encompasses the full breath of Australian retail, from family-owned small and independent businesses, comprising 95 per cent of our membership, to large national and international retailers supporting communities across metropolitan and regional Australia. With more than 155,000 retail outlets nationwide and a growing online presence, the retail sector is embedded throughout the economy, playing a critical role in the supply chain of Australian businesses.

ARC advocates for polices and reform that drive growth, resilience, and long-term prosperity for Australian retail and the millions who rely on it.

General comments

ARC members are committed to compliance with the Australian Privacy Principles (APP), and support strong privacy protections for consumers, both instore and online. Our members recognise the need for robust protections for children and young people under 18 in online settings. Effective privacy regulation must be proportionate and risk based, targeting platforms which may pose a genuine risk to privacy. A blanket approach risks misallocating compliance burdens without achieving the objective of protecting privacy.

E-commerce services are increasingly being chosen by all types of consumers to purchase goods. In 2025. 9.8 million Australian households purchased goods online, spending $82.6 billion online, equivalent to approximately 24% of all retail spending. Driven by value, convenience and choice, some consumers only purchase online.[1]

Retail e-commerce services, such as online supermarkets and marketplaces, are general audience websites geared towards consumers seeking everyday items such as groceries, clothing and household goods. Often, they complement physical stores by offering almost identical products for sale and applying the same controls and restrictions on products that may be unsafe or harmful or are age restricted. Consumers, including children and young people, can browse these public sites without logging in or registering (passive access). When browsing these general audience sites, minimal personal information is collected, no social interaction occurs and the identity of the user is unknown.

When considering the privacy risks posed by these retail services to children and young people, ARC recommends the OAIC apply a tiered risk management model that distinguishes between general audience websites and higher risk services that potentially may involve greater privacy harm. A risk-based approach of this

[1] *Australia Post eCommerce Report 2026.* Available at: https://auspost.com.au/content/dam/ecommerce-report/australia-post-ecommerce-report-2026.pdf.

Level 29
31 Market Street
Sydney NSW 2000

kind is not only proportionate but would, in ARC's submission, better achieve the underlying privacy objective of the Code without capturing services operated by retailers and other entities that do not pose a genuine risk to privacy.

This tiered approach would concentrate the most demanding obligations where the privacy risk to children is greatest, while ensuring baseline protections apply proportionately across the broader digital environment. For this reason, general-audience services, including everyday retail services, should be expressly excluded from the most onerous obligations under the Code.

ARC recommends the Code be reconsidered and recalibrated toward a tiered, risk-based framework.

Detailed comments about the Code

Our detailed comments regarding the Code are included below. Overall, in our view, several obligations in the Code are ambiguous, duplicative and disproportionately burdensome. In addition to our comments below, we recommend that entity obligations be structured as follows:

- Narrow application — Obligations relating to age assurance, consent, the best interests of the child standard, and data destruction should apply only to services with a high concentration of child users, or where a service is designed for or manifestly attractive to children.
- Broad application — Foundational obligations such as transparency requirements, Privacy Impact Assessments and staff training may appropriately apply to a wider set of services likely to be accessed by children.

1. Section 2 -Commencement and implementation period

We submit that a meaningful implementation period is essential to the practical success of the Code. A rushed transition risks producing superficial compliance or the blanket exclusion of children and young people from online services to avoid non-compliance. Such an outcome would be contrary to the Code's objectives.

We recommend a minimum implementation period of 12 months from the date of registration, with an implementation period of 24 months being preferable to allow organisations adequate time to undertake:

a. operational overhaul, including updates to internal governance frameworks, enterprise-wide staff training, and renegotiation of vendor and third-party data agreements;
b. comprehensive Privacy Impact Assessments across all digital assets within scope; and
c. significant technical builds, including if required, robust age-assurance mechanisms, data-mapping systems, and revised user consent journeys, without compromising existing system stability or security.

2. Sections 5 and 7 - Scope of the Code

As noted above, the Code is too broad and creates significant regulatory uncertainty for entities operating general audience websites. With children and young people routinely interacting with digital technology, the *"likely to be accessed by children"* threshold in sections 5 and 7 applies to everything online, regardless of whether the service is designed for, directed at, or actively used by children.

Level 29
31 Market Street
Sydney NSW 2000

As recommended above, applying a risk-based approach, the Code would:

a. Strictly apply to services that are intentionally directed at children or are primarily concerned with children's activities, not merely services that may be visited by children
b. Differentiate between services covered and obligations imposed based on the design and presentation of the services, the nature of the goods offered, existing account eligibility settings, marketing approach and whether a service operator knowingly identifies users as children.
c. Require low-risk services to meet minimal or no substantive requirements beyond the initial child privacy risk assessment.
d. Reflect that, as noted in the explanatory memorandum, older minors who engage with these services typically possess the maturity and digital literacy to navigate them without the additional protections the Code is designed to provide. This would avoid placing an unnecessary burden on entities to differentiate between older (16 and above) and younger.

In the event *"likely to be accessed by children"* test is retained, ARC calls on the OAIC to issue clear guidance on test. This is a critical threshold question and without this clarity, entities lack the certainty required to assess whether the Code applies to them and their compliance obligations. Consistent with the points made above, passive access by children or young people under 18 should not trigger the full obligations of the Code. ARC is available to work with the OAIC to develop this guidance.

3. Section 8 - Age assurance

Requiring all services *"likely to be accessed by children"* to conduct age assurance before collecting personal information is inconsistent with data minimisation principles and creates security risks given that entities will accumulate significant verification data. Age assurance should be reserved for services that pose a genuine privacy risk to children and young people.

For online retail, where a service complies with age restrictions on products, requires an adult payment method, has rules or policies indicating that the service is not intended for children, does not advertise to children, and removes known child accounts, additional age verification forces unnecessary data collection to address a negligible risk.

4. Section 9 - *"Strictly necessary"* default data collection standard

For online retail, the *"strictly necessary"* standard creates uncertainty around features that benefit the customer experience but are not required for bare product delivery. Product recommendations, fraud prevention signals, and service improvement analytics make services safer and more useful without creating privacy harms. Under a *"strictly necessary"* test, these features could be challenged despite clear benefit and negligible risk.

We recommend that the OAIC clarify, in guidance accompanying the Code, that *"strictly necessary"* encompasses the delivery of the full value proposition the user has enrolled in. For example, under a loyalty programme, personalised recommendations may be provided and information beyond bare transactional data is collected. ARC is available to work with the OAIC to develop this guidance.

5. Sections 10 and 11 - Best interests of the child standard

Level 29
31 Market Street
Sydney NSW 2000

The Code should expressly recognise, consistent with the approach taken in the *Age Appropriate Design Code (UK)*, that commercial interests are not inherently incompatible with the best interests of the child.

In addition, given the *Privacy Act* review has proposed a "fair and reasonable" test for the handling of personal information, we recommend the OAIC ensure the *best interests* standard under this Code is conceptually aligned with that proposed framework.

6. Section 15 – Consent Currency

We recommend the mandatory 12-month re-consent requirement be replaced with a periodic reminder model. Annual reminders could give children and young people and their parents or guardians an opportunity to review and update privacy settings, without requiring affirmative re-consent where settings remain unchanged.

7. Section 20 – Child Assent

Given the protections provided in sections 10, 11 (child's best interests) and 13 (parental consent), we submit that the dual-step requirement for both child assent and parental consent is unnecessary. This additional process adds complexity without a clear corresponding privacy benefit

8. Section 39 – Register of Privacy Impact Assessments

The requirement to publish a public register of PIAs should be removed. No comparable jurisdiction mandates this. The OAIC's power to access PIAs on request provides adequate oversight without the risks.

9. Section 33 - Shared household accounts and notification requirements

We submit that the Code should clarify how these notification requirements apply in shared household account environments, for example, where a family shares a digital wallet or retail account. Mandatory alerts to children in these contexts could produce notification fatigue in low-risk environments and may inadvertently interfere with legitimate and appropriate parental supervision. We recommend that the OAIC provide guidance addressing shared account scenarios. ARC is available to work with the OAIC to develop this guidance.

10. Sections 38 and 39 - Privacy Impact Assessments and the public register

ARC supports the requirement in section 38 for entities to conduct Privacy Impact Assessments. However, we submit that the requirement in section 39 to publish a public register of PIAs online is unnecessary and disproportionate. No comparable jurisdiction currently mandates this. In our view, the Commissioner's existing power under section 39(3) to access any PIA on request provides adequate regulatory oversight.

Conclusion

We appreciate the opportunity to provide feedback on the draft Code. We support the Code's objectives and believe that targeted, proportionate regulation, focused on services that present genuine child privacy risks, will be more effective than uniform obligations applied without regard to an actual risk profile.

AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

We welcome further engagement with the OAIC on these matters and are available to discuss our submission at the Commissioner's convenience. We would specifically welcome engagement with the OAIC regarding the development of guidance to the Code.

Please direct any queries in relation to this submission to our policy team at policy@retail.org.au.