BCA
Business Council of Australia

12 June 2026

[redacted]
Director, PRISM Taskforce
Office of the Australian Information Commissioner
Via email

Dear [redacted]

The Business Council of Australia (BCA) welcomes the opportunity to provide comment to the Office of the Australian Information Commissioner (OAIC) on the draft Children's Online Privacy Code (the Code).

The BCA's members comprise around 130 of Australia's largest employers who provide services every day to millions of Australians, including many children.

Over recent decades, business investment in privacy controls, awareness, and compliance frameworks has grown significantly, in recognition of community expectations around the collection, use, and protection of personal information, as well as evolving legal obligations. Our members recognise that privacy is a core element of their brands and their relationships with their customers.

The privacy frameworks established by each of our members are reflective of not only Australian legal requirements, principally the *Privacy Act 1988*, but also international jurisdictions in which our members operate, and specific requirements and expectations of their own customers.

As the BCA has previously submitted,[1] there are enormous opportunities for young Australians that come with digital engagement and digital literacy. Mindful of this, the Code should not inadvertently create regulatory barriers that hinder the development of innovative and beneficial online services for children or increase compliance costs by so much that services exclude under 18s from the service, which goes against principles of digital inclusion for young people.[2]

As drafted, the Code could also limit the ability of businesses to protect the safety and integrity of their systems, or conflict with regulatory requirements that are not explicitly in law. The BCA is also concerned the Code could easily introduce new risks, such as those arising from the collection of additional personal information to verify an individual's age or from mandated privacy default settings that may inadvertently increase exposure to fraud or scams. Compelling additional data collection – including on sensitive information like familial relationships – runs counter to the stated privacy objectives of the Code.

[1] See: https://www.bca.com.au/reports-submissions/submissions/submission-to-oaic-childrens-online-privacy-code-issues-paper/
[2] For example, OAIC Issues Paper of June 2025 stated "The aim of the Code is not to prevent children from engaging online, but to ensure their personal information is protected within that space."; and UN Convention on the Rights of the Child specifies "States parties should take all measures necessary to overcome digital exclusion." General comment No. 25 (2021) on children's rights in relation to the digital environment.

GPO Box 1472
Melbourne VIC 3001
www.bca.com.au

T 03 8664 2664
F 03 8664 2666
reception@bca.com.au

Key recommendations

In summary, the BCA's key recommendations are as follows, with details in remainder of this submission:

- The Code should be more closely aligned with the UK's Age Appropriate Design Code (AADC),[3] and Australian privacy law, consistently with the mandate to the OAIC for the Code.
- The Code should take a risk-based, proportionate approach to obligations.
- The Best Interests of the Child (BIOC) test should be an overarching framework rather than a test that applies on every collection, use and disclosure of personal information.
- The existing "reasonably necessary" test in Australian Privacy Principle (APP) 3 should be retained rather than imposing a new "strictly necessary" test.
- The concept of "likely to be accessed by children" needs to be defined and narrowed.
- Secondary use of personal information should continue to be allowed when it meets the BIOC test.
- Age assurance should be risk-based, data minimising, and proportionate.
- The Codes' approach to consent should follow Australian privacy law which is based on notice rather than consent, consistent with international settings.
- The Code should permit de-identification of information as an alternative to destruction.
- A 24-month implementation period is needed.

In relation to the first point, international alignment is important for businesses, particularly those that operate across multiple jurisdictions. Alignment with the UK's AADC would be consistent with the Australian Government Response to the Privacy Act Review, September 2023, Proposal 16.5: *"to the extent possible, the scope of the Australian Code will align with the UK Age Appropriate Design Code"*.[4]

The BCA's more detailed feedback is below.

Targeting of obligations to higher risk services

Many of our members provide online/app services to the general public – for example online retail, banking, search and cloud storage and online office applications. They are not child-oriented services, but have potential to be accessed by some children.

Nevertheless, the Code imposes uniform obligations on all covered services that meet the "likely accessed by children" threshold without regard to actual privacy risk to children. It fails to distinguish based on the nature or sensitivity of data collected, the purposes of use, or the likelihood of harm. An online retailer collecting limited personal information during a guest check-out for the purpose of delivery will be treated the same as a service posing high privacy risks to children.

One way to address this includes building in a risk-tiering system, where services that are low risk for child privacy harms (e.g. general-audience retail websites, online banking) are treated differently from those that are specifically targeted at children, attractive to children, and are used frequently by many children (noting we have proposed specific wording for "likely to be accessed by children" below).

A proportionate, risk-based approach, is absent from much of the Code. Proportionality is only considered in the context of what steps are "reasonable" to ascertain the age of an end-user, and not whether compliance obligations are proportionate to the privacy risks posed by a service.

[3] See: 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/
[4] See: https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

The BCA therefore requests the OAIC consider amending the Code so the most onerous requirements apply only to these child-focussed services that pose a high risk of child privacy harms.

The broader requirements could be applied to all services, whether or not they are targeted at children. This would include the requirements relating to transparency, privacy impact assessments and staff education and training, noting we also have comments on some of these requirements below. The "best interests of the child" standard could apply to all services, as long as it is implemented as an overarching principle as discussed below.

A risk-tiered approach would have some similarities with the codes and standards under the Online Safety Act,[5] where services deemed to be low risk have fewer obligations.

Section 6: Entities covered by the Code

We request the OAIC consider excluding other services, such as enterprise Designated Internet Services, on fair and objective criteria, on the basis these services should not meet the "likely to be accessed by children" threshold. As noted below there are significant difficulties with the potential scope of this test. Either this test should be substantially clarified and narrowed in operation, as noted below, or explicit carveouts should be provided so that enterprise services[6] and other applicable services based on fair and objective criteria are not required to assess whether they are covered in the first instance.

The BCA supports the retention of the health service provider exemption. Health providers are already subject to extensive regulation that would substantially overlap with the Code. The obligations under the Code are not appropriate for those entities. For example, requiring health service providers to re-obtain consent every 12 months (see s16(2)) could jeopardise ongoing treatment (noting we have broader comments on consent below).

Section 7: Likely to be accessed by children

The BCA requests the OAIC provides a tighter definition of the phrase "likely to be accessed by children" (see s7 and elsewhere). This is particularly important in relation to services that are not specifically targeting children but are provided to the general public.

As a specific suggestion, "likely to be accessed by children" could be expressly defined as services that are directed towards children; or the service is determined, based on reliable evidence regarding audience composition over a sufficiently long period of time, to be routinely accessed by a significant number of children.

The BCA also requests clarity about:

- the relative weight to be given to objective indicators such as the intended and actual audience, service design and presentation, number of child users in Australia (if known), marketing approach, account eligibility settings, whether users are knowingly identified or treated as children, whether the service's design is created to appeal to children, and whether terms or policies indicate the intended use by children.
- How incidental or passive access by children should be treated, including whether public accessibility alone is sufficient to bring a service within scope. Any public-facing website could in theory be accessed by children, and numerous apps as well, excepting those that are adult only.

Instead of a risk-tiered approach to the obligations, as discussed above, another approach is to have a tighter definition of "likely to be access by children" so that general audience services are excluded.

[5] The Online Safety Act standard for Designated Internet Services applies compliance obligations based on which risk tier a service falls under – there are three tiers.
[6] Services that are used internally in a business.

Section 8: Ascertaining age

The proposals in s8 of the draft Code go further than the social media minimum age law which only requires certain platforms to take reasonable steps to ascertain whether a user is under 16 or not. By contrast, under s8 of the draft Code, even low risk services would likely need to conduct some steps to ascertain a user's age. The BCA queries whether this is necessary, as this will encourage the over collection of a child's personal information, which may counterproductively result in a reduction in child privacy.

We instead submit that, similar to the UK's AADC, age assurance should be risk-based and proportionate. The approach should be interoperable with other Australian and overseas approaches, and expressly allow the use of existing data, and reuse of age assurance data collected under other regimes, to determine age without separate consent for reuse under each regulatory framework, to determine age.

The BCA also requests clarification of the OAIC's expectations for "reasonable" age verification measures in this section, especially where a service is not directed to children and does not knowingly handle children's personal information.

We request guidance on how the Code as a whole will operate when a business takes "reasonable steps" to determine a customer's age and treat customers consistently with their assessed age, but the assessment is later determined to be incorrect. In particular, given the business took "reasonable steps" to verify age, and this is a threshold test to determine whether the Code applies, we request guidance stating explicitly this should mean that the business has not breached the Code and is legally protected from action.

Similarly for the provisions that differ by age (eg s20), we request guidance stating a safe harbour applies to a business that takes "reasonable steps" but inaccurately determines a child's age.

Section 9: Strictly necessary collection of information

The obligation in s9 limits information collection to what is "strictly necessary". This concept is new in Australian privacy law and does not appear in comparable jurisdictions such as the UK, which will introduce uncertainty. It amounts to a new test/requirement that supplants Australian privacy law and jurisprudence built up over decades. This adds another layer on top of the existing requirement of "reasonably necessary", and been proposed without strong evidence and justifications. Further, the interpretation as proposed by OAIC excludes personalisation, recommendations, service improvement, and targeted advertising, which could inadvertently prevent beneficial data processing for children, including personalisation to provide age-appropriate content and safety and integrity measures.

The UK's AADC provides more flexibility on collection of personal information by permitting lower-privacy default settings if there is a 'compelling reason', having regard to the best interests of the child.

Given this, the BCA recommends the OAIC maintain the existing "reasonably necessary" test in APP 3. The separate "best interests of the child" (BIOC) requirement should provide adequate protection for children, and the "strictly necessary" requirement is not needed in addition, noting the comments we make below on BIOC.

More broadly, section 9 (collection and disclosure of (strictly) necessary information) overlaps to some extent with sections 10 & 11 (collection and disclosure in the best interests of the child). These sections use different tests on the same activity, causing complexity and difficulties in implementation. This issue would be significantly addressed by retaining use of the existing "reasonably necessary" test and avoiding adding the additional "strictly necessary" test.

Section 11: Secondary use or disclosure of information

Section 11 would effectively impose restrictions on secondary use or disclosure of information if consent has not been previously provided and the exemption for "authorised or required by law" has not been met

(many regulatory expectations or requirements are not in law as specific requirements). The Code as drafted could prevent various important uses of data relating to children.

For example, this could prevent banks from using a child's personal information for activities designed to address scams, fraud and security risks, which inherently protect all users including children. This is because such activities rely on complete customer population data to identify, and improve the identification of, patterns of scams and fraud that are not connected to the management of a specific customer's account. This includes fraud analytics rules, detection models and related initiatives which may use transaction markers, account behaviour, scam/fraud events and broader profile or network signals to detect suspicious activity and improve alerting for other customers. Where this data forms part of the broader population, any restriction on its use may reduce representation of the cohort and weaken overall detection capability.

It may also prevent social media services from providing age appropriate experiences to children. More importantly, it could prevent entities from using data from child accounts to identify risks that directly cause harm to children.

While consent may have been previously provided for some of these secondary uses, this prior consent would not occur for every possible secondary use which is why consent is very often not appropriate as a sole legal basis. The overall BIOC principle, with amendment as discussed below, will provide good protection for children and the additional restrictions are not required.

We therefore recommend the consent requirement be removed for use or disclosure of children's personal information for secondary purposes.

Section 10, 11: Best interests of the child (BIOC)

In relation to the BIOC test referenced in s10, s11 and elsewhere, the BCA recommends the OAIC takes an approach consistent with the UK AADC, with the BIOC being a holistic interpretative framework, rather than imposed as a mandate on every collection, use and disclosure, which goes considerably beyond the UK AADC. This is also arguably beyond the intent of the BIOC under the UNCR, which recognises BIOC as a concept that requires balancing of interests including digital participation.

Without this change, the draft COPC will require entities to assess every collection, use and disclosure against multiple tests: a new "strictly necessary" test, the existing "reasonably necessary" test, and BIOC creating confusion, difficulties in compliance, and opportunities for disputes to arise.

A holistic BIOC framework, in line with the UK AADC, along with a "reasonably necessary" test should be both sufficient and appropriate, because it is consistent with the APPs and includes an additional layer of child protection.

Regardless of any drafting changes to the Code, we specifically request guidance on how the BIOC test might apply to marketing. Direct marketing can include personalised/targeted services that provide unique value or more relevant offers to the particular customer, who may be a child, with such personalisation being consistent with the BIOC. We also request guidance on businesses using data to provide personalised offers or discounts to users under 18 such as through loyalty programs.

The BIOC test will operate in addition to existing and proposed obligations. This includes:

- the requirements relating to sensitive information;
- the 'best interests' test and acting 'efficiently, honestly and fairly' test in financial services; and
- the broader 'fair and reasonable' test proposed in the Privacy Act Review.

We recommend the OAIC ensure the BIOC test is conceptually aligned with these existing and proposed frameworks.

The BCA also recommends that the OAIC's guidance on the BIOC test acknowledges that an entity's commercial interests may not be incompatible with the best interests of a child. This has been helpfully acknowledged by the UK guidance on interpreting the BIOC under the UK AADC.[7]

Section 13: Age of consent

Section 13 states the minimum age for consent is 15. This means entities will need to age assure at both the 15 and 18 age boundaries. We note there are technological challenges in accurately assessing the 15 age boundary, similar to issues faced by the social media age ban. We also note this boundary differs from the age boundary of 16 used for the social media age ban, meaning some entities would need to collect granular age at multiple age boundaries in Australia.

Having a threshold age of 15 may create issues for services that customers under 15 will need to access. In some states, the minimum age of work is below 15 – in this case a child may be able to work but be unable to open a bank account without parental consent. This might also apply to other services related to work such as transport.

The BCA has concerns with the requirement to "take reasonable steps to confirm... parental responsibility" (s13(2)(b)) for children under 15. There would be very few, if any, publicly available data sets that would enable a business to verify two customers are in a parent-child relationship. There is no obvious and reliable way to verify this that would not involve the collection of extensive, very detailed and intrusive information about both individuals. This would not be consistent with the privacy-by-design ethos that the code purports to embody.

Residing at the same address would be a strong indicator, but this would not work for significant number of households, for example shared parenting arrangements. It is also unclear if a business can solely rely on residing at the same address, or if other indicators are required. This requirement could lead to businesses over-collecting personal information just to confirm parental responsibility, for example collecting both birth certificates (parent and child) as well as parent identification, with a need to store this sensitive information to demonstrate compliance.

Sections 13–19: Consent requirements

The approach in the Code, requiring consent in many circumstances, is out of line with both established Australian privacy law and international approaches. Other jurisdictions provide for other legal bases in addition to consent for collection of personal information.

The UK's AADC takes a different approach focussing on default privacy settings. The UK guidance states that consent is not inherently preferable to other bases for collection of data.[8] The Irish Fundamentals and the GDPR recognise consent as one of multiple equal legal bases, including legitimate interests and contractual necessity. The GDPR provides six equally valid legal bases for data processing, of which consent is only one.

In taking this approach that only permits the collection of personal information with consent, the draft COPC has removed a key balance from Australian privacy law between individual privacy rights and entities' ability to carry out their functions or activities, an objective of the Privacy Act. The Australian Privacy Act Review Report (2023) found that "an 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." (p3).

[7] **See:** 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/1-best-interests-of-the-child/
[8] **See:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/

Therefore the BCA recommends the OAIC take an approach on consent that is more aligned with existing APP principles and international settings, allowing multiple legal bases for processing of child personal information.

Given the number of apps and services that children can use, it could be burdensome and frustrating for children and parents to consent to the degree required by the draft Code.

In s15, there is a requirement for informed consent to cover a period of up to 12 months. We note no comparable jurisdiction, including the UK AADC or the Irish Fundamentals, imposes fixed-interval consent renewal requirements of this nature. A 12 month consent period could create consent fatigue, and be burdensome from an implementation perspective for entities. The prohibition on bundled consent in s14(3)(b) means some children/parents are likely to face numerous distinct consent requirements, each subtly different, heightening the consent fatigue.

The BCA recommends the OAIC consider replacing this with a requirement for a reminder notice to be issued every 12 months, once initial consent has been provided. This would allow children to reconsider and update their privacy settings should they wish to. This will allow the consent to remain valid until or unless the child decides otherwise.

If this change is not made, this would cause an issue when a child/guardian fails to take consent action – would the child lose access to the service immediately? It is unclear how this would work, for example, where a child has a bank account – would they be unable to withdraw their funds until they provide s15 consent?

We also request guidance on whether timeframes can apply where appropriate notification has been provided to the child/guardian and no action has been taken to withdraw consent.

Section 20: Assent of child

It appears the draft requires double consent for under 15s – by the parent/guardian (s13) and again by the child (s20). If the draft does not in fact impose this requirement, we recommend the guidance or explanatory materials make this clear.

However, if there is a double consent requirement, this would be burdensome for children, parents/guardians and businesses; disproportionate; and arguably unnecessary. It will also add to consent fatigue, reducing the value of consent requirements generally. It is not consistent with international practice in comparable jurisdictions, including under the UK AADC.

The BIOC framework plus the existing privacy protections make this double consent model unnecessary. Introducing a double consent/assent framework may raise additional challenges — for example, where a parent provides consent but the child does not, or vice versa, it is unclear how conflicts would be managed, or whether there would be a mechanism for challenge or escalation. This may also lead to (older) children seeking to remove parental oversight from services.

Another issue is that s20 may require a 4, 5 or 6 year old to "assent" to data processing after a parent has already given consent. This assent is unlikely to be meaningful or useful for this age group.

The BCA therefore recommends that any effective requirement for double consent be removed.

Section 32: Destruction of personal information

In Section 32, the draft Code includes the right for children to require destruction of personal information. We note the Productivity Commission's 2025 report recommended that a GDPR-style right to erasure should not be introduced in Australia[9] on the basis that compliance costs would outweigh privacy benefits. We also note there is no equivalent right for adults – such a right is not consistent with Australian privacy

[9] See final report, page 180.

law, and is not aligned with the UK AADC. As drafted, this requirement is likely to have unintended consequences, such as for the ability of services to retain and use data for safety and integrity purposes or for legal processes. These needs may not meet the strict tests for exemption such as being required by law or for an 'anticipated' legal proceeding.

This section would also create a right to require destruction of information owned or controlled by other individuals, including parents, which is problematic and may lead to misuse and impact the rights of other third parties.

We therefore recommend the OAIC also permit as alternatives:

- de-identification; or
- A UK-like model that has information as "put beyond use".

It is unclear why the OAIC has deemed de-identification as insufficient, when this has already been in use in Australian privacy law for decades.

Section 32(5)(a) explicitly states an entity is permitted to refuse a request for destruction (or alternatives above) if it is unreasonable to do so, an exemption we support. For consistency, this exemption should be included in the main exemption list in s32(3). This should also clarify that an exemption is provided where compliance is technically impossible or where requests are frivolous or vexatious.

Section 33: Geolocation notice

In the requirement for a geolocation notice (s33), the term "geolocation data" is not defined, and could therefore be interpreted broadly in ways that would require constant notification, which would greatly increase notification fatigue.

For example, with bank accounts, a parent can be notified about transactions. These notifications may reveal a child's location – for example if the physical location is in the seller's name, or there is only one of the seller (eg the Sydney Opera House).

This may mean a child needs to be notified every time they make an in-person transaction that their geolocation may be monitored, depending on how the requirement in s33(2) is interpreted (the child must be notified "throughout the period during which the monitoring is occurring"). This will be burdensome for both the child and the business, and will add to notification fatigue.

Section 39: Publication of privacy impact assessments

Section 39 requires entities to publish a register of privacy impact assessments. We understand this only means the publication of the title and date of the assessments, rather than the content of those assessments. We recommend guidance states this explicitly. Businesses would have significant concerns over a requirement to publish the full assessments as this would require the disclosure of competitively sensitive information.

Interaction with other frameworks

The BCA requests further guidance be provided on how the Code interact with existing or emerging child focused regulatory frameworks to promote consistency and regulatory clarity.

- The Code may overlap with other regulatory obligations, including the Scams Protection Framework. For example, any requirement that restricts the use of data, requires deletion, or enables a child to withhold consent to that use could potentially have adverse impacts on fraud/scam monitoring, link analysis, model performance, rule effectiveness, risk scoring, profiling, and the ability to protect other customers. Importantly, it may hinder efforts to prevent scams that directly target children.

- Further guidance is requested on how the Code interacts with the Australian Privacy Principles, including how obligations are intended to operate together. This includes the employee records exemption.

General comments

We request the OAIC provide detailed guidance in line with the guidance provided under the UK's AADC.

Specific guidance is requested on:

- Implementation timeframes, and compliance/enforcement during the transition period. We recommend an implementation period that is at least 24 months after the Code is registered.
  - The main risk of a short transition period is that organisations will simply exclude children from their online spaces entirely to avoid non-compliance. A 24-month period allows organisations to invest the necessary time and resources into the substantial operational, governance and technical changes required to safely engineer, test and implement required changes. The time required will depend on the final obligations in the code.
  - A 24 month implementation period does not substitute for addressing the issues noted in this submission that will be challenging to implement regardless of the transition period.
- Clarification of how the Code will apply to shared household accounts. For example, an account at a retailer that it used by multiple family members, including one or more children.
- The requirement to choose between age assurance or universal application of child level protections (see s8(5)), and the practical trade-offs this creates for services focussed on adults.

We would be happy to meet with the OAIC to discuss this submission. Please contact me on [redacted]

Yours sincerely

[redacted]

[redacted]
Executive Director, Policy
Business Council of Australia