Submission to the Children's Online Privacy Code exposure draft consultation — Office of the Australian Information Commissioner

About Middle Tech Australia

Middle Tech Australia brings together companies that occupy the space between start-ups and Big Tech. Our members build products that bring people together, enable conversations, creation and commerce, drive productivity, and support small businesses. Our aim is to be a constructive contributor to effective, evidence-based policymaking that supports investment and the services Australians rely on. We are committed to an open and innovative digital economy that works for Australian users, businesses, and the public interest.

The following principles guide our consideration of, and engagement with, the Office of the Australian Information Commissioner's Children's Online Privacy Code consultation:

1. **Proportionate and evidence-based:** Good regulation is calibrated to the actual risks and impacts of different products and services. Platform design, operating models, business size, and user characteristics all matter. Where new regulation is proposed, its objective and rationale should be clearly articulated and supported by evidence. Its definitions, thresholds, obligations, and penalties should follow from that objective, not from a one-size-fits-all template.

2. **Consultative, stable and predictable:** Good policy is made with the sector, not just for it. Middle-market voices are essential to good policy design, as they bring operational expertise on what it takes to build, operate, and scale digital services in Australia. Clear, stable regulatory frameworks support business planning and the investment needed to deliver digital services. Consultation should engage the full diversity of in-scope services early and transparently.

3. **Clear objectives, flexible means:** Effective regulation defines the ends it seeks clearly and specifically, then leaves industry room to determine how to meet them. Regulators and industry achieve more in partnership when the result is well-defined and the path to it is left open.

4. **Harmonisation, at home and abroad:** Australia's digital sector is governed by a growing number of overlapping instruments. Regulation should be coherent across them, and aligned with international standards where this reduces compliance burden and supports the objective of regulation. Coherence should be a design goal, not an afterthought.

5. **An open and competitive economy:** Australia's digital economy should enable companies of every size to compete, innovate, and grow. Open and competitive markets are best fostered when regulation is reflective of the nature and scale of the services it covers. It supports choice for Australians, lets companies invest in the tools and approaches best suited to their users, and helps them adapt quickly to emerging risks.

Executive summary

Thank you for the opportunity to make a submission to this consultation. Middle Tech Australia supports the Code's objectives and protective intent. The recommendations that follow are workability improvements designed to deliver the OAIC's intended outcomes proportionately across the diversity of in-scope services.

Our five recommendations are:

1. **Adopt reasonable and proportionate standards.** Replace "strictly necessary" (s9) with "reasonably necessary," reframe the "best interests of the child" test (ss10–11) as a holistic standard rather than a transaction-by-transaction one, and replace the s15(4)(b) 12-month consent cap with periodic privacy reminders.

2. **Reframe the consent architecture beyond the 12-month cap.** Recognise teacher- or school-mediated consent (s13), soften the s20 assent requirement, and address the s11(3) direct marketing rules.

3. **Further align with the UK Age Appropriate Design Code** where the OAIC has signalled it as the alignment target, including by adopting the UK's risk-based approach to age assurance (s8).

4. **Reduce the multiplicity of age thresholds** across the Australian regulatory stack, supporting a single coherent threshold across the Privacy Act, SMMA and related instruments.

5. **Remove the public PIA register (s39), clarify several operational drafting points raised by members, and set commencement at a minimum of 12 months**, with up to 24 for entities dependent on accreditation regimes that are not yet mature.

The supporting detail follows.

1. Reasonable and proportionate standards

1.1 "Strictly necessary" (s9)

The "strictly necessary" threshold is higher than the existing "reasonably necessary" standard, so we query whether it is appropriate for the Code to apply a higher standard than the one Parliament has legislated in APP 3. As drafted, the threshold may restrict data uses that materially benefit child users — including improvements to safety features, content moderation and fraud prevention, and analytics supporting core platform functionality. The threshold also sits in tension with safety features that depend on knowing whether a user is under a particular age: where personalisation supports safer or more age-appropriate experiences, it arguably is itself consistent with the child's best interests, and the two standards can pull against each other.

We propose replacing "strictly necessary" with "reasonably necessary," in alignment with APP 3, supported by interpretive guidance confirming that trust and safety, fraud prevention, content

moderation, and product improvements that materially contribute to safety or age-appropriateness are compliant uses.

1.2 Best interests of the child (ss10–11)

We believe the "best interests" standard will be difficult to operationalise consistently across different products, user bases and use cases. This introduces tension with other elements of the Code: collecting information that serves the child's best interests, for example for safety purposes, may not be "strictly necessary" for provision of the service. A service provider will never be in a position to understand the full context of an individual user, and this practical limitation must be reflected in what providers can be expected to do.

We propose reframing the test as "not against the best interests of the child" — a holistic standard applied across the Code rather than to discrete data-handling activities. This better aligns with how the principle operates under the UK AADC. We also propose codifying in the Code the Explanatory Statement's language that "an entity's commercial interests may not be incompatible with the best interests of the child," with worked examples.

1.3 12-month consent validity (s15(4)(b))

The 12-month consent cap, applied at the granular level Division 2 contemplates, will be a significant and onerous compliance requirement, particularly for small to medium service providers. We query whether this requirement would actually improve privacy outcomes for children online, or whether it could contribute to consent fatigue. The practical burden of repeated re-consent will fall on parents and carers, who would be required to repeat the process across multiple services and, in many cases, multiple children. The UK Information Commissioner's Office is presently reconsidering consent-heavy approaches in the cookie-consent context for closely analogous reasons, signalling international recognition of the consent-fatigue problem and a regulator-level rethink that the OAIC may wish to take into account.

As drafted, the Code could potentially require multiple different annual renewals for one company across various consent types, and we seek clarification on whether the 12-month cap is intended to apply to each and every category of consent, including consent at the point of creating an account.

We propose replacing the mandatory 12-month refresh with a requirement to send periodic, age-appropriate privacy reminders that highlight current settings and how to withdraw consent, with entities given flexibility to choose a reminder system that matches their user base.

2. Regulatory alignment, at home and abroad

It is encouraging to see some regulatory alignment between the Code and the UK Age Appropriate Design Code, and we would encourage further harmonisation with that Code, while noting the nuances of the Australian regulatory environment. Two areas warrant attention.

2.1 Age assurance (s8)

We encourage the OAIC to consider adopting the UK's approach to age assurance more fully. The standard in the UK Code is framed more flexibly and is concerned with tailoring protections by reference to children's differing ages and developmental stages, whereas s8 of the Code reads chiefly as an age-assurance gateway.

It is not clear in the draft whether a "low risk" service would not require age assurance at all. The OAIC's own age assurance technology guidance suggests low-risk services should consider whether self-declaration can be relied upon. We seek clarification on the circumstances that would be considered low risk.

Broad age assurance can itself create privacy harms by concentrating sensitive identity information — an outcome at odds with the Code's data-minimisation objectives and acknowledged in the OAIC's October 2025 SMMA privacy guidance.

We propose that s8 adopt the UK AADC's risk-based framing, with the obligation removed altogether for services presenting low or negligible child privacy risk. Existing controls under other Australian laws, including AML/CTF and KYC obligations, should also be expressly recognised as contributing to compliance. Where a service already establishes that users are above a relevant age threshold under another regulatory regime, duplicating that determination under a separate age-assurance regime serves no protective purpose.

2.2 Domestic harmonisation

Australia's digital sector operates across overlapping instruments with inconsistent thresholds. Three age thresholds now apply to online services in Australia: 15 for Code consent, 16 for the SMMA, and 18 for age-restricted content. In light of this, the proposed Code would add further complexity to an already complex legislative landscape, with so many layers of consents, expiring consents, dual child and parent assents, and multiple age boundaries that make consistent compliance challenging.

Our central concern is the multiplicity of inconsistent thresholds rather than any specific number. Alignment to a single threshold across the Privacy Act, SMMA, classification reforms and related instruments would reduce duplicative age-verification infrastructure and support a coherent Australian framework. The threshold of 16 already legislated under the SMMA has particular merit as a basis for that alignment.

We understand the OAIC has indicated it will cooperate with eSafety on aligning age assurance requirements across the respective legislative frameworks, and we encourage that work to extend to consent age and to a common definitional schedule.

3. Other feedback

The following are concrete drafting concerns where targeted clarification or amendment would materially improve workability across the diversity of services in scope.

3.1 Scope: services "likely to be accessed by children" (s7)

The s7 threshold captures a wide range of services that present limited or highly contextual child-specific privacy risks. The test conflates two distinct concepts: services likely to be accessed by children, and services likely to cause privacy harm to children. As drafted, "likely to be accessed" could be read as "able to be accessed" — a formulation that places no meaningful limitation on the services potentially captured.

We support codifying non-exhaustive factors for the assessment, drawing on UK ICO guidance, and including a carve-out for services not directed to or marketed to children and which have taken reasonable steps to restrict child users.

Services that present no meaningful child-specific privacy risk should not be drawn into the Code's full set of obligations by reason of the broad definitional categories alone.

3.2 Parental consent and assent (ss13, 20)

A threshold question arises as to whether the Code, as an instrument made under the Privacy Act, can validly require parental consent for the creation of accounts by users under 15. A requirement of that kind would expand the consent obligations Parliament has legislated rather than elaborate them, and a change of that significance is more appropriately a matter for the legislature than for a subordinate instrument. We therefore seek confirmation of whether s13 is intended to apply at the point of account creation, and, if it is, encourage the OAIC to consider whether that outcome falls within the scope of the Code-making power or is better addressed through primary legislation.

The technology to verify parental responsibility is not yet mature. The examples of reasonable steps in the Explanatory Statement are either highly susceptible to fraud from a child motivated to bypass the system (for example, email communication) or potentially intrusive with significant privacy risks (for example, vouching via a bank token or providing a form of government ID directly to a service provider). The s20 dual-step process requiring child assent in addition to parental consent is largely impractical for real-time features and will significantly slow processes down, leading to a suboptimal user experience.

We propose recognising account-level parental controls and teacher- or school-mediated consent as constituting parental consent for s13, and amending s20 so assent for younger children operates as an age-appropriate notice requirement, with active assent reserved for older children.

3.3 Direct marketing (s11(3))

The dual requirement in s11(3) that direct marketing is only permissible where consent is obtained and the use is in the best interests of the child goes well beyond existing privacy legislation and significantly limits a service's ability to promote features which could reasonably be expected to be enjoyed and welcomed by users. On a plain reading, direct marketing as drafted includes promotion of a service's own features. We propose that a distinction be drawn between cases where a platform is promoting its own services and cases where it is promoting advertisements on behalf of third parties.

3.4 Transparency (ss23–24)

The requirements that privacy policies be age-appropriate and incorporate non-text material mean that organisations will, in practice, need to publish multiple versions of the same policy. We seek clarification on which version would be relied upon in a dispute and how any discrepancies, perceived or actual, between versions would be reconciled.

3.5 Destruction (s32)

We support the right of children to request the destruction of their personal information. Section 32 as drafted goes beyond APP 11.2 by treating de-identification as insufficient. We propose permitting de-identification, including the OAIC's existing "beyond use" concept, as a compliance route where destruction is not technically feasible, with explicit exceptions for cyber security and fraud prevention, AML/CTF and Scams Prevention Framework obligations, and regulatory record-keeping. Guardrails are also needed to avoid frivolous or automated requests, and the Code should address the position of data already used to train AI models, which cannot feasibly be extracted from those models and destroyed.

3.6 Public PIA register (s39)

We support the s38 PIA obligation and the broader regulatory oversight PIAs enable. Public publication of the register, however, treats private entities as if analogous to public sector bodies, exposes commercially sensitive product roadmaps, and surfaces detailed control information that can be exploited by malicious actors, particularly controls relating to privacy, trust and safety, child safety, abuse prevention and security. We propose removing the public register requirement while retaining the OAIC's ability to request PIAs and any supporting register on a confidential basis, and seek clarification that the requirement, if retained in any form, refers solely to publishing a list of completed PIAs rather than the PIAs in full.

4. Commencement (s2)

We acknowledge that s2 is currently to be drafted. Implementation will require significant re-architecting across services, including consent flows, age assurance, data retention and destruction processes, and internal training. Several supporting technologies — parental consent providers, age assurance providers — are not yet mature.

We propose a minimum 12-month transition period, with provision for a longer transition of up to 24 months for entities whose compliance depends on supporting accreditation regimes that have not yet been established. Commencement should also be aligned to the milestones of related reforms, including OSA Part 4A and Phase 2 ARM Codes and the Unfair Trading Practices Bill, to avoid sequential and disruptive compliance cycles.

Conclusion

Middle Tech Australia supports the Code's objectives and the protective intent behind it. The recommendations in this submission are workability and proportionality improvements designed to

deliver the OAIC's intended outcomes across the diversity of in-scope services. We would welcome continued engagement.