Children's Online Privacy Code Stage 3 Consultation Submission | ICMEC Australia

Privacy (Children's Online Privacy) Code 2026 – Exposure Draft Review

Overarching position

ICMEC Australia strongly supports the *Privacy (Children's Online Privacy) Code 2026* as one part of a whole-of-system approach to keeping children safe online. The Code represents a very significant legislative advance for children's digital rights in Australia, and we commend the OAIC for its development.

ICMEC Australia's position is simple: privacy and safety must be operationally integrated, not treated as competing obligations. The Code's ultimate effectiveness will depend on whether its privacy protections actively reduce exploitation risk or inadvertently create gaps that harmful actors can exploit. The three priority issues outlined below are identified through that lens.

About ICMEC Australia

The International Centre for Missing and Exploited Children (ICMEC) Australia is a specialist not for-profit organisation that strengthens Australia's ability to prevent and respond to online and technology-facilitated child sexual exploitation and abuse. We operate at the intersection of frontline practice and national policy, helping governments and systems respond to rapidly evolving digital risks with practical, coordinated solutions.

Our work focuses on strengthening national capability where it matters most – supporting those who respond to child exploitation and abuse related harm first, while ensuring policy, regulation, and technology design are informed by real-world operational experience. One way we do this is by leading the SaferAI for Children Coalition, a coalition of government and non-government organisations, including the child protection sector, academia, and law enforcement, with the shared goal of ensuring that AI and emerging technology is adopted with safeguards to ensure child safety in the digital environment.

Priority issue 1: the privacy-safety nexus

The Code's data minimisation and erasure obligations (ss 11, 32–33) are sound in principle. However, as currently drafted, they create significant ambiguity at the interface with child sexual exploitation and abuse (CSEA) detection and law enforcement operations.

CSEA detection tools – including PhotoDNA and hash-matching technologies – depend on the retention of specific categories of data. A compliant platform under the Code may face obligations to delete precisely the data that is operationally critical for identifying victims, linking offending patterns, and supporting law enforcement referrals to the Australian Centre to Counter Child Exploitation (ACCCE). It is currently unclear how this may interact

with existing preservation obligations under the *Telecommunication (Interception and Access) Act 1979*.

Recommendations:

1. An express carve-out within ss 11 and 32–33 to preserving data necessary for CSEA detection operations and compliance with law enforcement preservation notices to make this operationally binding. Exploitation and abuse risk is currently limited to a discretionary consideration in the explanatory statement for s 10.
2. Guidance that clarifies the overlap with the preservation obligations under ss 107H–107M of the *Telecommunication (Interception and Access) Act 1979* (Cth), with preference to preserving data that may be material to investigations.
3. Inclusion of a mandatory reporting mechanism to the Australian Centre to Counter Child Exploitation (ACCCE) or NCMEC for CSEA-related data prior to erasure.

These recommendations ensure that the privacy obligations under the Code operate only to protect children from harm, and cannot be exploited by offenders and malicious actors.

Priority issue 2: AI applications and emerging harms

The Exposure Draft is largely silent on artificial intelligence. This is a significant gap given the pace at which AI is being weaponised for CSEA, including AI-generated abuse material, sexual extortion at scale, AI-driven grooming, and harms directly derived from interaction with AI models. Findings from ICMEC Australia's SaferAI for Children Coalition document these as current – not merely emerging – threats.

Particular concern attaches to the rapid popularisation of AI companion applications and generative chatbots that deploy features such as persistent memory, emotional modelling, and simulated attachment to sustain user engagement. On platforms lacking robust age assurance and content guardrails, these design features can produce interaction dynamics that functionally replicate grooming and exploitation – including the cultivation of trust, emotional dependency, and the elicitation of personal disclosure – without any human offender being present. The data from early 2025 showed that more than 70% of teens had used AI companions, most being regular users, and children under 13 are increasingly engaging with the platforms. The Code's current silence on these risks is a material omission.

Recommendations:

1. Require mandatory Privacy Impact Assessments (PIAs) for any AI-driven processing of children's data, including behavioural profiling, recommendation algorithms, and generative features – consistent with the UK Age-Appropriate Design Code's DPIA requirement.

2. Address the erasure of children's data used in AI training datasets, which the current drafting does not reach, and which poses distinct harm vectors beyond conventional data retention.
3. Expressly include AI services – including AI companion applications and generative chatbots – within the definition of services likely to be accessed by children under Part 2 of the Code and the accompanying explanatory statement.

Priority issue 3: "best interests" must be operative, not aspirational

Section 8 of the Exposure Draft establishes that an entity must act in the best interests of the child when handling children's personal information. This is the Code's foundational standard, and is substantiated in the Explanatory Statement which articulates seven considerations, including child exploitation risks, developmental impacts, and the evolving capacities of children across age and maturity. As currently drafted, these considerations are discretionary and hold no operative legal force – neither a company, nor the Commissioner, are bound to apply the considerations. Other Commonwealth legislative instruments take the approach of codifying the factors which must be considered when assessing the best interests of the child.

Secondly, the Explanatory Statement states "an entity's commercial interests may not be incompatible with the best interests of the child." The statement cites the UN Convention on the Rights of the Child (UNCRC) as the source of the factors that may be considered in determining the best interests of the child. However, the UNCRC Committee on the Rights of the Child, in General Comment No. 25 (2021) – which compliments General Comment no. 14 – states unequivocally that the best interests of the child should be "a *primary consideration* when regulating advertising and marketing addressed to and accessible to children." ICMEC Australia acknowledges the Code's intention to give effect to this standard, but submits that the current drafting does not ensure it is consistently operative in practice.

To ensure that the best interests of the child do not become subsidiary to commercial interests, the Code and Explanatory Statement should clarify an entity's obligations where the best interest of the child and commercial interests genuinely conflict.

Recommendations:

1. Elevate the seven factors in the Explanatory Statement to mandatory considerations on the face of the Code, consistent with other legislative instruments of the Commonwealth.
2. Amend the Code and Explanatory Statement to clarify an entity's obligations where its commercial interests conflict with the best interests of the child.

Conclusion

ICMEC Australia supports the *Privacy (Children's Online Privacy) Code 2026* and commends the OAIC's commitment to world-leading protections for children in digital environments. The recommendations above are offered in the spirit of strengthening an already significant reform.

Striking the right balance between privacy and safety is the defining implementation challenge. A Code that treats privacy and child safety as complementary – rather than competing obligations - will be a genuinely transformative instrument.