Submission to the Office of the Australian Information Commissioner Exposure Draft: Privacy (Children's Online Privacy) Code 2026

Industry, Civil Society and Academic Consultation Track

5 June 2026

Digital Defence is an Australian not-for-profit organisation working to create online safety in Australia through law reform, enforcement reform, and digital literacy education. We engage with federal policy, regulators, and parliament on the architecture of online harm regulation. We submit these comments in response to the exposure draft of the Privacy (Children's Online Privacy) Code 2026 (the Code).

Digital Defence supports the development of this Code. Strong, enforceable privacy protections for children online are overdue and necessary. We make these comments constructively, as participants in the broader process of building a regulatory framework that works for children, for platforms, and for the Australians the law is designed to protect.

Our submission addresses three concerns. Each reflects a structural issue that, if not resolved, risks the Code producing the pattern Digital Defence has documented across Australian online safety regulation more broadly: obligations on paper, without the operational architecture to make them real.

1. The enforcement architecture

The Code imposes detailed obligations on entities in relation to age verification, data minimisation, consent, destruction, and privacy impact assessments. These are well designed obligations. The question the Code does not answer is what happens when they are not met.

The Office of the Australian Information Commissioner's (the OAIC) existing powers under the Privacy Act are complaint driven and slow. Digital Defence has documented the gap between complaint volumes and enforcement outcomes at the eSafety Commission across multiple schemes where obligations accumulate, complaints accumulate, and enforcement does not follow at the pace or scale needed to change platform behaviour. The OAIC's complaint based enforcement model under the Privacy Act reflects the same structural limitation.

Digital Defence submits that the Code should be accompanied by an explicit, published enforcement framework that sets out:

- the categories of conduct that will attract priority enforcement attention,
- the timeframes within which the OAIC will respond to complaints about Code breaches,
- the civil penalty regime applicable to Code contraventions, with graduated consequences sufficient to change platform behaviour.

Laws are only as good as the enforcement of them. A code that imposes meaningful obligations without a credible enforcement pathway does not protect children. It creates the appearance of protection.

2. The 'best interests of the child' standard

Sections 10, 11 and 38 make the best interests of the child the overriding test for collection, use, disclosure and privacy impact assessment. Digital Defence supports this as a principle. It is, however, left without definitional content.

Without a statutory definition or harm based taxonomy, the standard vests discretion in entities to determine what the best interests of the child require in any given situation. Entities facing commercial pressure will apply the standard to produce compliant looking outcomes. Regulators will face difficulty enforcing it against entities that can point to a documented internal assessment, however thin. Courts will face interpretive uncertainty.

Digital Defence submits that the Code or its accompanying explanatory statement should supply, at minimum:

- a non-exhaustive list of factors that must be considered in assessing best interests, drawing on established child rights frameworks;
- examples of conduct that is presumptively inconsistent with a child's best interests (profiling for commercial targeting, geolocation disclosure to third parties, manipulation of interface design to increase data sharing); and
- a clear statement that commercial interest is not a consideration that can outweigh the best interests of the child.

A framework that leaves harm undefined does not protect children. It delegates the determination of harm to the entities whose commercial interests are engaged in making it.

3. Age verification and the data minimisation tension

Section 8 requires entities to take steps that are reasonable in the circumstances to ascertain the age of end users before collecting personal information. Section 9 requires data minimisation by default. These two obligations are structurally in tension.

In practice, reliable age verification requires the collection of additional personal information such as government-issued identity documents, biometric data, or device and behavioural signals that are themselves sensitive. The Code is silent on how this tension is to be resolved. An entity complying with section 8 by implementing document based age verification may simultaneously be collecting sensitive information that section 9 is designed to prevent.

Digital Defence submits that the OAIC should issue guidance, before the Code commences, on the permissible methods of age verification and the privacy constraints that apply to each. That guidance should address:

- the destruction obligation that applies to identity information collected for verification purposes (the Code already addresses this in section 8(4) for sensitive information; clarity is needed for non-sensitive identity information);
- whether third party age verification services that retain data for their own purposes are permissible; and
- the minimum data principle as applied to age verification specifically.

The Code should not inadvertently create a new and significant data collection event as the price of compliance.

Conclusion

Digital Defence supports the Code as a meaningful step toward enforceable privacy protections for children online. Our comments are directed at ensuring the Code functions in practice, not only on paper. The three structural concerns we have identified, being enforcement architecture, definitional content for the best interests standard, and the age verification data tension, are each resolvable. We urge the OAIC to address them before the Code is finalised.

Digital Defence welcomes further engagement with the OAIC on any of the matters raised in this submission.

[redacted]

Co-founder and CEO, Digital Defence

socials@digitaldefence.org

5 June 2026