



To:



[OAIC - COPC](#)

Subject:

Submission on the Children's Online Privacy Code Issues Paper

Date:

Thursday, 4 June 2026 1:45:20 PM

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear OAIC,

Thank you for the opportunity to provide feedback on the Children's Online Privacy Code Issues Paper.

I strongly support the objective of improving privacy protections for children online. Children face unique risks in digital environments and deserve clear, meaningful protections against excessive data collection, profiling, targeted advertising, inappropriate disclosure of personal information, and security breaches.

However, I am concerned that some approaches being considered, particularly those involving age verification or identity verification, may create unintended privacy risks for both children and adults.

Requiring users to provide government-issued identification, biometric information, or other sensitive credentials in order to access online services risks creating large new repositories of highly sensitive personal information. Such systems may increase the consequences of data breaches and identity theft while undermining the privacy rights of all Australians. In many cases, the process of verifying age may require the collection of more personal information than the service would otherwise need to collect.

I encourage the OAIC to ensure that the Code does not create incentives for widespread identity verification, mandatory collection of government identification documents, or routine biometric processing as a condition of access to online services.

Instead, I recommend that the Code prioritise privacy-protective alternatives, including:

- High privacy settings by default for all users or all users reasonably likely to be children.
- Data minimisation requirements that limit collection, use, retention and disclosure of personal information regardless of a user's age.
- Restrictions on profiling, behavioural advertising and geolocation tracking where children may be present.
- Child-friendly transparency requirements and consent mechanisms.
- Risk-based service design that assumes uncertainty about age and applies stronger privacy protections without requiring identity verification.
- Privacy-preserving age assurance technologies that provide only an age range or eligibility result and do not disclose identity or retain additional personal information.

Where there is uncertainty about a user's age, it may be preferable to apply child-protective privacy standards by default rather than requiring users to prove their identity. Such an approach would better align with privacy-by-design principles and reduce the amount of personal information collected across the digital ecosystem.

I also encourage the OAIC to consider how the Code can strengthen privacy protections for all Australians. Many of the concerns raised by children—including excessive data collection, complex privacy notices, manipulative consent processes, and pervasive tracking—are concerns shared by adults. Measures that improve transparency, data minimisation, security, and user control would deliver broader public benefits while supporting the primary objective of protecting children.

Thank you for your consideration.

Kind regards,

A solid black rectangular box used to redact the signature of the sender.