QUEENSLAND Family & Child Commission

Queensland Government

Telephone: 07 3900 6000
Reference:

Ms Elizabeth Tydd
Australian Information Commissioner
Office of the Australian Information Commissioner

Via email:

Dear Ms Tydd

I appreciate the opportunity to provide feedback on the Office of the Australian Information Commissioner's (OAIC) Draft Children's Online Privacy Code (the Code).

This submission approaches privacy regulation as a core element of a broader child safeguarding system, beyond technical compliance alone. For children and young people, privacy, safety, and protection from exploitation are inseparable. Findings from the Queensland Child Death Review Board's *In Plain Sight: A system response to child sexual abuse* (IPS report) demonstrate that digital environments can amplify offender reach, enable concealment, and contribute to systemic failures to identify and disrupt harm. Children should be able to participate in digital environments without trading safety or privacy for access. The Code therefore has an important preventative function in reducing exposure to exploitation and coercion and should be interpreted and applied in that context.

Children's engagement with digital environments does not fit neatly within fixed service categories, and the Code's protective purpose should not be constrained by narrow definitions that risk excluding emerging or hybrid models. I support a broad, purposive application of the Code to social media services, relevant electronic services, and designated internet services, consistent with its development under the *Privacy Act 1988* (Cth) and its operation alongside the *Online Safety Act 2021* (Cth).

The Commission remains available to provide further information and welcomes ongoing engagement with the OAIC throughout the consultation process. If you would like to discuss this matter further, please don't hesitate to contact me directly on XX or via email at XX.

Yours sincerely

Luke Twyford
Principal Commissioner
Queensland Family and Child Commission
June 2026
Strengthening the "Best Interests of the Child" test (Section 10)

Level 8, 63 George Street
Brisbane Qld 4000
PO Box 15217
Brisbane City East Qld 4002

Telephone: 07 3900 6000
Facsimile: 07 3900 6050
Website: qfcc.qld.gov.au
ABN: 91 102 013 458

The Commission considers that strengthening section 10 would provide greater clarity by explicitly requiring entities to prioritise children's physical, psychological, and developmental safety over commercial interests or service functionality.

This is consistent with National Principles for Child Safe Organisations (National Principles) which require organisations to create environments that minimise risk and actively promote children's safety and wellbeing.[1] It also reflects the findings of the IPS report that child safety must be the paramount consideration across all legislative and regulatory frameworks.

To operationalise this requirement, the "best interests" test should explicitly require entities to assess how platform design may increase a child's vulnerability to grooming, coercion or exploitation, including:

- anonymity and pseudonymity features, which reduce accountability and enable offender concealment
- recommender systems and engagement optimisation algorithms which may progressively expose children to higher-risk content or contacts
- encrypted and private communication channels, which allow interactions to move beyond visible or moderated environments, bypassing parental oversight
- emerging artificial intelligence (AI) and gaming environments, including the use of generative AI to simulate peers and automate grooming behaviours.

Consistent with the IPS report, harm often arises from a sequence of escalating engagements rather than a single interaction. The Code should require entities to assess and disrupt these pathways as a core component of best interests' compliance.

Age assurance as prerequisite for meaningful protection

Services likely to be accessed by children should implement age assurance measures proportionate to the risk profile of the service. Without this, obligations relating to consent, data minimisation and best interests are unlikely to be meaningfully applied in practice. The burden of verification should not fall solely on children, or their carers, and age assurance mechanisms should be designed to minimise additional privacy risks.

Privacy by default as contextual prevention (Section 9)

The Commission supports the "high privacy by default" and data minimisation requirements in Section 9 as structural safeguards that reduce opportunities for harm, rather than technical compliance-preferences. Consistent with the National Principles and Queensland's *Child Safe Organisations Act 2024* (Qld), organisations have an affirmative duty to design environments that minimise the opportunity for children and young people to be harmed.

Just as physical services must eliminate spaces where perpetrators can isolate children, digital platforms must eliminate the digital blind spots created by excessive data collection. Collecting only strictly necessary information reduces the intelligence available to perpetrators for profiling, targeting, and grooming.

---

[1] Australian Human Rights Commission. 2018, *National Principles for Child Safe Organisations*

Privacy protection must, however, be understood in context including privacy from whom. Children are most vulnerable when they are alone, isolated and invisible: when harmful behaviour cannot be detected or disrupted by those responsible for their safety Data must be able to flow appropriately to support protection.

Privacy settings and data minimisation must be balanced with the need for appropriate information sharing and system visibility to support safeguarding. Requiring children to actively opt in to optional data handling practices supports agency, consistent with National Principle 2.

Ensuring privacy protections support safeguarding and information sharing

A critical finding of the IPS report was that offending often persisted because information remained siloed and warning signs were never fully connected.

The Code should ensure that privacy protections do not unintentionally impede appropriate information sharing, and that platforms are not legally or procedurally discouraged from sharing intelligence about potential groomers or high-risk algorithmic patterns with law enforcement and the proposed Child Safeguarding Intelligence Hub, recommended in the IPS report.

Section 11(2) of the Code provides exceptions for disclosure to *promote justice* or respond to *serious threats*. The IPS report indicates that these exceptions must be operationally workable. Many grooming indicators are sub-threshold - individually insufficient for a criminal investigation, but, in aggregate, revealing clear predatory intent. The Code's interpretative guidance clarifies that sharing such intelligence with authorised safeguarding authorities is consistent with the "best interests of the child" test.

Consistent with Transformational Recommendation 3 of the IPS report, the Code should support a shift to proactive information exchange and a safeguarding ecosystem that anticipates risk rather than merely reacting to harm.

Algorithmic accountability and emerging digital risks (Section 28)

Evidence from the IPS report indicates that automated decision-making and recommender systems can accelerate a child's exposure to harmful content and facilitate contact with offenders—dynamics often invisible without deliberate, safety-focused scrutiny. In light of these risks, more prescriptive standards are needed to govern the design and operation of these systems.

Privacy impact assessments should explicitly evaluate escalation pathways, the role of anonymous interaction features in enabling offender concealment, and the potential for recommender systems to increase exposure to grooming or exploitation.

A rapidly emerging threat identified in the IPS report is the use of AI-powered chatbots by perpetrators to automate grooming, to simulate the tone, style and interests of a child's peers to build trust at scale. The eSafety Commission's March 2026 Transparency Report[2] found popular AI companion chatbots were failing to protect Australian children from

[2] eSafety. 2026, *Responses to transparency notices: Artificial intelligence services*

sexually explicit content. A 2026 eSafety Commission survey of 1,950 children aged 10 to 17 years in Australia, found 79 per cent of children had used an AI companion or assistant.

The Code must require platforms to assess and mitigate the risk of their conversational AI features being used for such deceptive purposes.

Strengthening erasure and recovery pathways for Victim-Survivors (Section 32)

For children who are victim-survivors of image-based abuse, the permanence of digital material represents ongoing harm. The Code should therefore include robust erasure pathways. Section 32 should ensure destruction processes are expedited, trauma-informed, and designed around the experience of the child rather than platform compliance architecture.

De-identification alone is insufficient given the high risk of re-identification through cross-referenced datasets; actual destruction is required.

In line with Operational Recommendation 11 of the IPS report, the Commission recommends the Code facilitate alignment with international initiatives like Project Arachnid. In a poll of 1,624 Australian's aged 13-17, commissioned by the OAIC, 92 per cent supported the Code creating an enforceable right to erasure.

Accessible Justice: Child-friendly complaints (Section 36)

The IPS report highlights that children and families frequently experience reporting systems as fragmented, inaccessible, and adult-centric. In response, more prescriptive standards are needed to ensure inquiry and complaint processes are genuinely child friendly.

The Code should mandate processes that are easy to locate, navigate, and trust from a child's perspective, with safe and developmentally appropriate pathways to raise concerns.

I acknowledge the OAIC's parallel consultation with children and young people and consider it important that the final Code's explanatory statement clearly demonstrates how those perspectives materially shaped the design of section 36. I also consider that section 36(4), which permits anonymous or pseudonymous complaints, is an important safeguard.

Conclusion

I recognise the Code as a meaningful step toward embedding child safety and privacy protections within Australia's digital regulatory framework, with the potential to operate not merely as a compliance instrument but as a genuine preventative safeguard against exploitation, coercion, and harm in digital environments.

In finalising the Code, priority should be given to:

- interpreting scope broadly and purposively to capture emerging and hybrid service types, consistent with the *Privacy Act 1988* and the *Online Safety Act 2021*
- strengthening the "best interests of the child" test to explicitly prioritise children's physical, psychological and developmental safety, including risks arising from platform design and recommender systems
- establishing proportionate age assurance expectations that are effective without introducing additional privacy risks

- requiring algorithmic accountability measures that explicitly address grooming, exploitation, and escalation pathways
- ensuring privacy protections enable, rather than impede, proportionate information sharing for child protection, law enforcement, and online safety purposes
- providing expedited, trauma-informed erasure pathways for victim-survivors of image-based abuse
- mandating accessible, child-centred complaints processes aligned with children's needs and developmental capacity
- demonstrating how children's and young people's views have shaped the final Code and its explanatory materials