[redacted]

[redacted]

Office of the Australian Information Commissioner
GPO Box 5288
Sydney
New South Wales 2001

Dear Commissioner,

I write to formally submit my response to the Exposure Draft of the Children's Online Privacy Code 2026 and the accompanying Explanatory Statement.

I commend the Office of the Australian Information Commissioner for its work in developing this important Code. Strengthening privacy protections for children in the online environment is both timely and necessary, and I strongly support the intent and direction of this initiative.

[redacted]

My submission is informed by both policy considerations and practical, real-world observations of how children interact with digital services. Since 2016, I have spoken with over half a million Australian juveniles and have grown to become one of Australia's most prominent experts in the areas of Cyber Safety and Internet Awareness.

In my submission, I have sought to highlight a number of key areas where further clarification or strengthening of the Code may assist in ensuring its objectives are effectively realised in practice. In particular, I have focused on issues relating to age assurance, consent, data minimisation, and the practical application of the "best interests of the child" principle.

I appreciate the opportunity to contribute to this consultation process and would welcome any opportunity to provide further input or clarification if required.

Please find my submission attached.

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

TABLE OF CONTENTS

[redacted] [redacted]

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

1. INTRODUCTION

I welcome the opportunity to provide a submission on the Exposure Draft of the Children's Online Privacy Code 2026 (the Code).

I have worked for close to two decades in the field of cyber safety and online harm prevention, including extensive engagement with schools, parents, law enforcement, and young people across Australia. My work focuses on educating children and adolescents about online risks, digital behaviours, and the real-world consequences of technology use. Since 2016, I have spoken with over half a million Australian juveniles and have grown to become one of Australia's most prominent experts in the areas of Cyber Safety and Internet Awareness.

Through this work, I have observed first-hand how children interact with online platforms, how personal information is shared and exploited, and the practical limitations of existing privacy and safety frameworks. I have first hand and extensive experience of where juveniles are falling down online and the risks they are taking, especially within Social Media and Online Gaming environments.

This submission is informed not only by policy considerations, but by lived, real-world experience of how children engage with digital services and is representative of someone who has been working at the coal-face of juvenile online harm for a considerable amount of time.

2. OVERALL POSITION

I strongly support the intent and objectives of the Children's Online Privacy Code.

The Code represents a necessary and important step toward strengthening privacy protections for children and aligning Australia with international developments in this space. It reflects the proactive steps Australia is taking in protecting Australians from risk and harm, when many other countries are failing.

In particular, the emphasis on the following points is both appropriate and well overdue:

- Privacy by default.
- Data minimisation.
- The best interests of the child.
- Increased transparency.

However, the effectiveness of the Code will ultimately depend on how well it translates into real-world environments used by children. There is a significant risk that, without further clarification and strengthening in key areas, the Code may be implemented in a way that satisfies compliance requirements without meaningfully improving outcomes for children.

3. KEY ISSUES and RECOMMENDATIONS

3.1. Age Assurance (Section 8)

The Code adopts a risk-based approach to age assurance, allowing flexibility in how entities determine the age of users. In practice, this is one of the most challenging aspects of online safety, because children routinely:

- Misrepresent their age to access platforms.
- Use shared or parent accounts.
- Circumvent age gates with relative ease.

[redacted]

Self-declaration mechanisms, in particular, are widely ineffective and should not be relied upon for services that present higher risks. In practice, simply asking a user to enter their age or confirm that they meet a minimum age requirement does little to prevent underage access.

Children quickly learn that these systems can be bypassed with ease, and it is common for them to misrepresent their age in order to access platforms, features, or peer groups that would otherwise be restricted. This behaviour is not typically driven by malicious intent, but by curiosity, social pressure, or a desire to participate in the same digital environments as their peers.

From a design perspective, self-declaration offers minimal friction and no meaningful verification, making it one of the weakest forms of age assurance. It places the burden of compliance on the child, rather than on the service provider, and assumes a level of honesty and risk awareness that does not align with developmental realities. As a result, platforms may technically satisfy age-related requirements while continuing to expose children to environments and risks that are not appropriate for their age.

For higher-risk services, such as those involving direct messaging, geolocation, behavioural profiling, or interaction with unknown users, reliance on self-declaration is particularly problematic. In these contexts, inaccurate age information can directly increase the likelihood of harm. A more robust, risk-based approach to age assurance is therefore required, one that reduces reliance on self-declaration and incorporates additional safeguards proportionate to the level of risk involved.

At the same time, more robust age verification methods introduce their own privacy risks, including the collection of sensitive identity information. Data collection and storage is a constant concern for many parents and many modern juveniles are becoming increasingly suspicious of how and where their data is being collected and retained by Social Media platforms in particular.

Recommendations:

- Establish minimum baseline requirements for age assurance in higher-risk services.
- Prohibit reliance on self-declaration alone for services involving profiling, direct messaging, or geolocation.
- Require independent evaluation or auditing of age assurance mechanisms.
- Provide clearer regulatory guidance on acceptable age assurance practices.
- Ensure the continual development and use of age verification and assurance systems where data storage is not required, and digital information is not retained.

3.2. Best Interests of the Child (Sections 10 and 11)

The requirement that collection, use, and disclosure of personal information be consistent with the "best interests of the child" is a critical and a welcome inclusion. However, the concept is not sufficiently defined in operational terms.

Without clear guidance, there is a risk that entities interpret "best interests" narrowly, or in ways that align with commercial objectives such as engagement and growth. Within the recent Social Media Age Restriction legislation, the term "*reasonable steps*" has evolved a tokenistic response by certain platforms, leading them to take a less active approach to the legislation.

This is particularly problematic in environments where platform design is inherently optimised to maximise user attention. As such, wording should be robust and direct to ensure more effective levels of compliance, especially when the safety and protection of children is the goal.

Recommendations:

- Provide a clear framework or criteria for assessing "best interests".
- Require entities to document and justify decisions where this principle is applied.
- Align the interpretation with established child development and wellbeing principles.
- Consider requiring independent oversight for high-risk determinations.

3.3. Data Minimisation and Privacy by Default (Section 9)

The requirement that only "strictly necessary" personal information be collected by default is a strong provision. However, the concept of what is "strictly necessary" is highly subjective and open to broad interpretation.

In practice, many platforms may argue that extensive data collection is necessary to support core functionalities such as personalisation, recommendation systems, or advertising models. These functions are often framed as integral to the user experience, enabling content discovery, relevance, and platform usability.

Such claims can blur the distinction between what is genuinely necessary to deliver a service and what is commercially advantageous to the provider. As a result, data collection that primarily supports engagement optimisation or revenue generation may be characterised as "essential," despite not being required for the core operation of the service.

From a child safety perspective, these same mechanisms are frequently where the greatest risks arise. Personalisation and recommendation systems rely on the continuous collection and analysis of behavioural data, which can lead to profiling, prolonged engagement, and exposure to increasingly targeted or extreme content.

Advertising models incentivise deeper data collection and tracking, often across multiple services, creating detailed digital profiles of children over time. These practices can reduce a child's autonomy, limit their exposure to diverse content, and increase vulnerability to manipulation or exploitation.

Without clear boundaries, there is a risk that the concept of "necessity" is interpreted in a way that normalises high levels of data collection, rather than minimising it. Strengthening guidance around what constitutes "strictly necessary" is therefore essential to ensure that child privacy and safety are prioritised over commercial interests.

Recommendations:

- Provide clearer guidance on what constitutes "strictly necessary".
- Identify and specify categories of data collection or processing that should be restricted or prohibited for children under all circumstances.
- Require entities to specifically justify the necessity of each category of personal information collected and the reasons behind such collection.
- Introduce stronger safeguards around profiling and behavioural tracking of children.

3.4. Consent Framework (Division 2)

The Code sets out robust requirements for consent, including that it must be informed, voluntary, specific, and unambiguous. While these are appropriate and well-established principles in privacy law, they do not adequately reflect the behavioural reality of how children engage with digital services.

In practice, the conditions required for meaningful consent are rarely met in environments designed for speed, convenience, and engagement. Consent is typically obtained at moments where children are focused on accessing a service or feature, not on understanding complex data practices or long-term implications.

In my experience working with young people over the past 25 years, children do not read privacy policies, and even when they attempt to, they often lack the context or developmental capacity to fully understand them.

Consent mechanisms are frequently presented in ways that are abstract, text-heavy, or disconnected from the actual experience of using the platform. At the same time, children are highly responsive to interface design. Visual cues, button placement, colour, and language can strongly influence decision-making, often nudging users toward accepting data practices without genuine consideration. This creates an environment where consent can be shaped or steered by design, rather than freely and deliberately given.

As a result, consent in its current form often provides limited meaningful protection for children. It risks becoming a procedural step that legitimises data collection, rather than a safeguard that empowers informed choice. Without additional measures such as simplified, context-driven explanations, restrictions on manipulative design practices, and stronger defaults, there is a significant gap between the legal standard of consent and the reality of how it operates in practice for children.

Recommendations:

- Prohibit the use of manipulative design practices in obtaining consent.
- Require child-friendly, standardised consent formats that are not complicated.
- Introduce friction or additional safeguards for higher-risk data uses.
- Require testing of consent mechanisms with children to ensure comprehension

"Friction" refers to the deliberate introduction of additional steps, safeguards, or decision points that slow down or interrupt a user's ability to provide consent, particularly where the consequences of that decision may not be fully understood, or where the risks are elevated.

In the context of children, friction is not a barrier to access, but a protective mechanism designed to address:

- impulsive decision-making,
- limited understanding of long-term consequences,
- susceptibility to persuasive or manipulative interface design.

At present, many digital services are designed to minimise friction in order to maximise engagement and data sharing. This creates an environment where children can consent to complex data practices with little awareness or reflection. Introducing friction in higher-risk scenarios helps ensure that consent is more deliberate, informed, and meaningful.

3.5. Transparency and Age-Appropriate Communication (Division 3)

The requirement to provide "age-appropriate" information is important, particularly the baseline assumption of comprehension at the 10 to 12 age range. However, in practice, many entities may satisfy this requirement through minimal adjustments to existing privacy policies.

Children require information that is simple, visual, contextual and immediately understandable. Traditional privacy policies are typically presented as long, static documents that users are expected

to read and understand at the point of account creation or first use. In practice, these documents are rarely read by adults, and are even less accessible to children.
As a result, static privacy policies do not support meaningful understanding or informed decision-making by children, especially pre-teens.

Just-in-time notifications are contextual, they are real-time prompts that appear at the moment a user is about to engage with a feature or action that involves the collection, use, or disclosure of personal information.

Rather than expecting users to recall information from a policy read earlier (or not at all), just-in-time notifications provide:

- immediate relevance,
- contextual clarity,
- timely decision support.

Children engage with digital services in a highly interactive and immediate way. Their decisions are often rapid and impulsive, influenced by interface design and made without revisiting prior information. Expecting a juvenile to rely on a previously presented privacy policy is unrealistic and does not reflect how children learn or process information.

Just-in-time notifications align with how children actually interact with technology by delivering information at the point of need and simplifying complex concepts into actionable guidance whilst also reinforcing learning through repetition.

Recommendations:

- Mandate the use of layered, visual, or interactive privacy explanations.
- Require usability and comprehension testing with children.
- Introduce measurable standards for readability and accessibility.
- Encourage the use of just-in-time notifications rather than static policies.

3.6. Right to Erasure (Section 32)

The inclusion of a right to request the destruction of personal information is strongly supported. However, in practice, deletion is often incomplete or unclear.

Data may continue to exist in backups, third-party systems, and derived datasets or profiles, even after a deletion request has been made. In many cases, organisations retain copies of data in backup and archival systems for operational resilience, security, or compliance purposes. While these systems serve legitimate functions, they can result in personal information being retained well beyond the point at which a user believes it has been deleted.

Similarly, where data has been shared with third parties such as analytics providers, advertisers, or cloud services, it may remain outside the direct control of the original entity, limiting the effectiveness of any deletion request.

In addition, modern digital services routinely generate derived or inferred data based on user behaviour, including profiles, preferences, and predictive insights. Even if the original data is deleted, these derived datasets may persist and continue to influence how a child is treated or what content they are shown.

From a user perspective, particularly for children and their parents, there is an expectation that deletion is complete and final. Where this is not the case, it creates a disconnect between

[redacted] [redacted]

expectation and reality, potentially undermining trust and limiting the practical effectiveness of the right to erasure.
Children and parents are unlikely to understand the limitations of deletion. The Code should strengthen the practical operation of the right to request destruction of personal information by requiring greater transparency, clearer scope, and strict steps to address data held by third parties and in derived forms.

Without such measures, there is a risk that deletion rights will not meet user expectations or effectively mitigate harm, particularly in the context of juveniles. Children are becoming increasingly concerned about where their data is going, and this is an important consideration.

Recommendations:

- Require entities to clearly communicate the scope and limitations of deletion.
- Extend deletion obligations to third parties where feasible.
- Require confirmation of deletion in plain, accessible language.
- Consider stronger requirements around the deletion of inferred or derived data.

3.7. Enforcement and Compliance

A key risk for the Code is that it becomes a compliance exercise rather than a driver of meaningful change. In practice, regulatory frameworks in the digital environment are often implemented in ways that satisfy formal requirements without materially improving outcomes for users.

Entities may adopt a "tick-box" approach, updating policies, introducing consent prompts, or making minor adjustments to disclosures while maintaining underlying data practices that continue to expose children to risk. This is particularly likely where commercial incentives, such as data monetisation and user engagement, are in conflict with principles like data minimisation and privacy by default. As a result, there is a real risk that entities may comply with the foundations of the Code, whilst undermining its intent.

This challenge is compounded by the fact that many risks to children arise not from written policies, but from platform design. Default settings, interface choices, and user flows that encourage data sharing or limit meaningful understanding are the biggest concerns. From a child's perspective, privacy is shaped by what the platform does, not what the policy says.

To ensure the Code delivers meaningful protections, oversight and enforcement must focus on real-world outcomes, including whether measures are effective, understandable, and aligned with the best interests of the child. This should include mechanisms such as independent auditing, user-centric testing, and greater transparency around data practices.

Without such measures, there is a significant risk that compliance will be procedural rather than protective.

Recommendations:

- Introduce requirements for independent audits of compliance
- Require transparency reporting on children's data practices
- Establish clear penalties for systemic or repeated breaches
- Provide sufficient resourcing for regulatory oversight and enforcement

4. THE IMPORTANCE OF REAL-WORLD CONTEXT

It is critical the final Code reflects the realities of how juveniles use technology. Teens and pre-teens do not engage with digital services in a structured or policy-driven way. Their behaviour instead, is

[redacted]

shaped by a complex interaction of platform design, peer influence, ease of access, and developmental factors.
The environments in which children operate are highly dynamic, visually driven, and engineered for engagement, often encouraging rapid decision-making with limited reflection. Features such as default settings, prompts, rewards, and notifications can significantly influence behaviour in ways that prioritise participation and data sharing over caution or privacy.

In addition, children are strongly influenced by their peers and social norms, particularly in online spaces where connection and inclusion are highly valued. This is particularly apparent in Social Media. The desire to belong or participate can override risk awareness, leading to behaviours that may not align with their best interests.

This is compounded by the ease with which digital services can be accessed and navigated, often with minimal barriers or safeguards. Importantly, children are still developing the cognitive and emotional capacity to understand long-term consequences, assess risk, and make informed decisions.

Any regulatory framework that does not take these factors into account risks being ineffective in practice, as it may rely on assumptions about user behaviour that do not reflect how children actually interact with technology.

5. CONCLUSION

The Children's Online Privacy Code 2026 represents a vital step toward strengthening protections for Australian children in the digital environment. Its principles of privacy by default, data minimisation, transparency, and prioritising the best interests of the child are both necessary and welcome. In principle, the Code aligns Australia with international developments and demonstrates a proactive commitment to safeguarding juveniles online.

However, as this submission has outlined, the effectiveness of the Code will ultimately be determined by its real-world application. Without clear operational guidance, robust risk-based measures, and a strong focus on implementation, there is a significant risk that the Code may satisfy compliance requirements in form but fail to achieve meaningful protection for children in a practical sense.

Children's engagement with digital services is immediate, dynamic, and socially driven. They do not interact with platforms through policy documents or abstract principles. Their behaviour is shaped by design, peer influence, and developmental capacity. Mechanisms such as self-declared age, consent forms, and static privacy policies, while legally necessary, are often insufficient in protecting children from harm. Similarly, data collection practices justified as "necessary" for functionality can, in practice, prioritise commercial objectives over child wellbeing.

To be truly effective, the Code must bridge the gap between legal standards and the lived realities of children online. This requires clear operational definitions of concepts such as "best interests of the child" and "strictly necessary" data. Risk-based safeguards, particularly age assurance, consent, and high-risk features are also very important considerations as well as child-centred design regarding consent and information mechanisms, including interactive, just-in-time notifications.

Ultimately, the goal of the Code should be to create environments where children can engage online safely, with privacy and autonomy protected, and where digital platforms are accountable for designing with children's best interests at the forefront. Ethical Design and/or Safety by Design principles are what I have been advocating for almost two decades and I will continue to push for this as the foundation of the Code.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Areas of Expertise

- Child online safety & digital literacy education.
- Cyber safety mentoring & school programs.
- Risk assessment in social media & online gaming.
- Age-appropriate communication & consent design.
- Policy advisory on digital privacy frameworks.

[redacted]

[redacted]

[redacted]

[redacted] prioritises the best interests of children, focusing on practical, real-world solutions that reflect how young people actually engage with technology. His recommendations are grounded in direct experience, evidence-based practice, and a deep understanding of developmental psychology, platform design, and digital risk.

Impact Snapshot

- 500,000+ juveniles educated and mentored nationally.
- Active engagement with schools, parents, and law enforcement across Australia.
- Longstanding contributor to national policy discussions on cyber safety and online privacy.

[redacted]