Submission on the Proposed Children's Online Privacy Code

From: Pixevety Pty Ltd
Date: 31 July 2025
To: Office of the Australian Information Commissioner

Introduction

As an Australian EdTech small business, Pixevety welcomes the opportunity to respond to the OAIC's consultation on the proposed Children's Online Privacy Code. We are a data protection award-winning Australian EdTech provider specialising in K-12 school media safeguarding, supporting schools in compliance to securely manage and protect student media in a way that aligns with privacy legislation, institutional policies, and family expectations. We hope our submission offers the OAIC a practical perspective drawn from our experience in the privacy and commercial space, including the operational challenges the Code may pose for small businesses. It is also hoped this submission also highlights the importance of supporting those organisations committed to doing the right thing – prioritising child safety and fostering responsible, ethical innovation.

Pixevety has been serving Australian schools for over a decade. Our media consent-driven platform is built on privacy-by-design principles, ensuring that privacy and security are integrated into every stage of development. We help schools empower students and parents to regain control over how their digital media is handled by providing clear, explicit consent tools automated at scale. We prevent metadata harvesting, online profiling and behavioural tracking, and all media sharing is restricted to verified, school-authorised users through strict access and permission controls. Additionally, data is minimised, encrypted, and stored securely, with regular privacy reviews and audits to ensure compliance with the highest international privacy and security standards.

As a K–12 contracted service provider (data processor) purpose-built to support compliance, we strongly support the Code's aim to enhance online privacy protections for children. By strengthening the Australian Privacy Principles (APPs) under the Privacy Act, the Code will empower EdTech providers and other online services to confidently develop world-class, privacy-by-design tools for children, while fostering a fair and competitive environment for both local and global EdTech companies.

However, we wish to raise several practical and evidentiary concerns that, if unaddressed, may impact the Code's effectiveness and proportionality, especially in an educational setting.

1. Strengthen the Evidence Base Before Finalisation

We heartily support the inclusion of youth voices to "ensure that the Code reflects the real experiences and needs of children and their families", however, note that key positions shaping the Code appear to be based off a single piece of youth research (a panel survey) involving a relatively small sample of 1,624 panel respondents. While we acknowledge the value of this research, we are concerned that relying heavily on one piece of search with a sample of this size, particularly where participants are self-selecting (although the methodology is unclear) does not provide a sufficiently representative or behaviourally grounded foundation of data for regulatory design. We understand similar criticisms have been raised in relation to the eSafety Commission's recent consultations regarding the social media ban for children, where it emerged that adults – not children – were completing surveys intended to capture children's experiences on social media. This highlights the

broader risk of drawing regulatory conclusions from flawed or unverified datasets, and underscores the urgent need for a more robust, transparent, and child-centred evidence base before finalising the Code.

Our understanding of the UK market is that the UK ICO undertook more robust research across various key stakeholders. We recommend complimenting this existing research with behavioural analytics, education system insights and academic research to inform proportionate design.

Recommendation:
We respectfully suggest that the OAIC supplement existing research with broader behavioural data, platform analytics, academic evidence, and cross-sector consultation, particularly with educators, schools, and technology providers working directly with children in structured environments.

2. Ensure Proportionality Based on Context and Purpose

The Code should distinguish between commercial services and institutional contexts, such as schools, which are governed by public obligations, regulated consent frameworks, and child protection mandates.

"My ambition for children is for them to be able to learn and develop safely online, benefitting from every advantage available to them with the risks removed. Every child should believe their safety is being ***prioritised in the same way it is at school*** *or in the local park with the knowledge that they are safe from harm."* **– Children's Commissioner of England**

In fact, the UK ICO prepared Code guidance specifically for EdTech and it is hoped the OAIC will do the same.

As a service provider that operates exclusively in educational settings, we urge the OAIC to differentiate between services that target children for commercial purposes, and those that serve an educational, civic, or public interest function.

Many EdTech providers already operate under strong contractual, technical, and organisational safeguards, often acting as data processors under the direction and control of schools or educational institutions. Many, like Pixevety, have also invested heavily in achieving formal certifications such as ISO/IEC 27001 or equivalent standards. The Code must recognise these realities to avoid overregulating the wrong party or duplicating existing controls.

The current draft appears to adopt a one-size-fits-all approach that could impose disproportionate compliance burdens on privacy-conscious platforms such as ours, while doing little to shift practices among larger commercial entities.

Schools are not unregulated entities. They operate under robust legislative and policy controls centred around child safeguarding and protection. The Code should recognise this existing compliance environment and avoid duplicative or conflicting obligations.

Within schools, it is also important that the Code distinguishes between EdTech tools directly used by children for learning and engagement, and those used by school administration to support legitimate interests such as compliance, safeguarding, and operational management. While student-facing tools focus on education delivery, administrative tools often handle data for regulatory obligations and school governance, which may require different privacy considerations and data retention practices. For example, certain personal

data may need to be retained by a school for legitimate safeguarding purposes related to school operations, and beyond a student's enrolment to meet archival and educational record-keeping obligations.

Recommendation:
Over the course of 13 years of schooling (Kindergarten to Year 12), an Australian child spends approximately 15,600 hours at school, with various EdTech tools being used directly by these children for several hours per day. We believe education is a distinct category and a vital piece of the Code's puzzle that warrants broader consultation within the Code. We recommend strengthening the evidence base for this critical sector before the Code is finalised.

Introduce context-sensitive obligations, and ensure the Code distinguishes between:

- Platforms with commercial intent (e.g. ad-driven social media),
- Platforms used in a supervisory highly regulated environment (e.g. schools), and
- Platforms with demonstrable privacy-by-design foundations supporting administration and compliance.

The Code should clarify how it interacts with settings where parental authority or institutional duty of care governs decision-making, such as school enrolments, student management systems, or safeguarding platforms.

3. Clarify How Consent and Capacity Should Be Managed

The absence of a clear definition of consent in the Australian Privacy Act contributes to ongoing ambiguity in the draft Code, particularly in relation to how consent should be applied in different contexts. In practice, schools typically operate within institutional consent frameworks set by education departments, parent agreements, and school policies, rather than relying on direct digital consent from the child. This highlights the need for the Code to account for the operational realities of institutional environments like schools, where alternative and often more robust safeguards are already in place.

Institutional consent should work in tandem with age-appropriate engagement of the child, particularly older cohorts. Regulators globally appear to be reevaluating the reliance on consent as the primary mechanism for safeguarding personal data, particularly in regard to children's data and complex or high-risk contexts. For example, the UK ICO has stated: "Reliance on consent as a lawful basis for processing children's personal data is often inappropriate, especially where there is a power imbalance or where children may not fully understand what they are consenting to." (Source: ICO, Age-Appropriate Design Code, Section 3: Best interests of the child).

Neuroscientific research confirms that the human brain - particularly the prefrontal cortex, which governs impulse control, future planning, and decision-making - continues to develop until approximately age 25. This area is central to an individual's ability to understand risks and consequences, weigh trade-offs, and form informed judgements. (Source: Simply Psychology – Prefrontal Cortex Development)

While young people, especially those aged 13–17, should absolutely be supported in exercising digital rights and privacy agency, it is important to acknowledge that their legal capacity to give fully informed consent is not absolute – particularly when faced with

complex, abstract, or hidden data practices such as algorithmic profiling, third-party sharing, or use of machine learning for at scale safeguarding.

In school settings, consent frameworks already recognise this developmental nuance. Institutional consent is typically managed by education authorities or guardians, with student engagement designed to be age-appropriate, scaffolded, and protective by default.

Moreover, the requirement to obtain "developmentally appropriate consent" from children aged 13 to 17 must be carefully balanced with legal guardianship responsibilities and school policies. While it is vital to empower all children with digital rights, this should not come at the expense of parental authority or institutional safeguards. Schools must have a clear understanding of their obligations to ensure compliance – and be held accountable when they fall short.

While supporting children's right to be heard is important, the Code must recognise that many data decisions do involve complex trade-offs that require adult-level reasoning. In these cases, true protection does not come from asking children to consent or configure privacy settings, it comes from embedding safeguards by design, default, and institutional responsibility.

Recommendation:
Provide practical implementation guidance for different service types. This includes how to align the Code's expectations with institutional consent mechanisms in school settings and how to manage layered consent between child, guardian, and school.

We respectfully recommend that the Code avoid placing sole responsibility on children to navigate privacy terms or data practices they may not be developmentally equipped to understand, particularly within the context of their own educational environment.

- Reinforce the 'best interests of the child' principle as a primary design filter, rather than over-relying on consent as a legal mechanism.
- Encourage a **layered approach to consent**, recognising the roles of parents, schools, and service providers in supporting and scaffolding young people's privacy rights.
- Ensure that any requirements around obtaining child consent align with developmental science and the intent of APP 3 and APP 5, which focus on *necessary* and *appropriate* collection and notification, respectively.

Other areas of concern:

- The new Code must clearly distinguish between the responsibilities of data controllers and data processors, ensuring Code obligations are appropriately assigned based on who determines the purpose and means of data processing.
- While the Online Children's Code provides a valuable framework for enhancing child privacy protections, it may present significant compliance challenges for smaller EdTech companies. Start-ups and niche providers often lack the dedicated legal, cybersecurity, and compliance teams that larger organisations have and will require greater support and guidance from the OAIC. The cost and complexity of aligning with advanced privacy-by-design requirements (e.g., implementing data minimisation, robust access controls, and ongoing audits) may discourage innovation and reduce the diversity of privacy-conscious tools available to schools. Support measures such

as clear implementation guidelines, affordable privacy toolkits, or a phased compliance approach could help smaller providers meet the Code's expectations without compromising competitiveness or innovation. We hope to see 'privacy-by-design'/'privacy-by-default' practices become standard across Australia.

- The Code would benefit from further guidance on how to apply the "best interests of the child" test in everyday school operations, especially where operational needs (e.g. managing media permissions, protecting images) intersect with data protection duties.
- The Code should ensure that its obligations are proportionate to the size, function, application and risk profile of the organisation, particularly when dealing with public sector, educational or not-for-profit entities whose primary mandate is child welfare.
- The Code should reinforce that accountable system design, privacy by default, and prevention of misuse are stronger safeguards than reliance on child or parent consent alone.

Conclusion

Pixevety strongly commends the OAIC's intention to strengthen children's privacy online. However, to be effective, the Code must:

- Be grounded in diverse and robust evidence that reflects the realities of different sectors and application contexts,
- Recognise the role of context and purpose in digital service design,
- Offer clear and practical guidance on managing consent, and
- Account for the legitimate interest of safeguarding in institutional environments.

While the UK's Children's Code made important strides toward child-centred data protection, its shortcomings include over-reliance on consent, ambiguous scope, one-size-fits-all requirements, and limited accommodation for non-commercial, institutional contexts. These issues offer valuable lessons for jurisdictions like Australia seeking to implement a balanced, more effective children's code.

We remain available to participate in any further consultation or working groups and would be pleased to contribute our specialist knowledge in image safety and school-based digital privacy practices.

Submitted by:

[redacted]