Submission: Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 – Treatment of School-Directed Safeguarding EdTech Services

From: Pixevety Pty Ltd

Date: 3 June 2026

To: Office of the Australian Information Commissioner

Introduction

We appreciate the ongoing opportunity provided by the Office of the Australian Information Commissioner (OAIC) to contribute to the development of the Online Children's Code through submissions and participation in roundtable consultations.

As a proud, award-winning in privacy-by-design, trusted Australian-owned and developed privacy compliance solution to schools, Pixevety strongly supports the Australian regulator's clear commitment to placing the best interests of children at the centre of the proposed Online Children's Code. Establishing a framework that prioritises children's privacy, safety, and wellbeing by design is both necessary and timely, particularly given the increasing role digital services play in young people's lives. We welcome the emphasis on accountability and higher standards for services likely to be accessed by children and recognise the important role the Code can play in lifting baseline protections across the ecosystem.

At the same time, we encourage the OAIC to take careful consideration of the diversity of technologies, data and deployment contexts captured within the scope of the Code, particularly where services operate in controlled environments such as schools or are designed with privacy-enhancing, purpose-limited functionality.

The Exposure Draft does not, from an operational perspective, strike the right balance between strong privacy protections and practical workability. It's expanded scope, that goes beyond similar enacted Codes overseas, particularly for services operating in school-authorised contexts, risks creating uncertainty and disproportionate compliance burdens.

While consent may be appropriate for optional or discretionary services, it is often neither practical nor suitable where technology is used to fulfil a school's legal, ethical, and safeguarding obligations to students. In such circumstances, requiring consent risks undermining the very protections the Code seeks to promote.

The Code should recognise that schools and their service providers may need to process personal information, including sensitive information, where appropriate safeguards exist, when such processing is necessary to protect children, manage educational environments, prevent harm, or fulfil statutory obligations.

For this reason, it is essential that the Code goes beyond general risk-based language and provides explicit recognition and a clearly defined pathway for such low-risk, privacy-preserving services. This should include a form of scoped application, exception, or tailored treatment within the Code to ensure these technologies are not subject to disproportionate or inappropriate requirements. Without this, there is a real risk that innovation in privacy-enhancing products will be chilled, adoption will be undermined, and children will ultimately be worse off as a result, considering what is actually happening in schools today.

Importantly, this submission is not an argument for reduced regulatory standards. All services must remain fully subject to Australian privacy law and core data protection principles. Rather, it is a call for the Code to be sufficiently precise and nuanced to ensure that its application reflects real-world risk and does not unintentionally penalise models that are demonstrably aligned with its underlying objectives. Failure to maintain this distinction risks imposing disproportionate obligations on services that enhance, rather than undermine, children's safety and privacy.

Greater Clarity on Code Thresholds and Provisions

Not all online products and services present equivalent risk profiles to children or operate under the same incentives. For example, technologies that minimise data collection, operate solely under institutional instruction, and avoid secondary uses of data, are fundamentally different from consumer-facing, data-driven services. Without clear differentiation in the Code, there is a risk that these lower-risk, privacy-protective solutions are inadvertently constrained, or misunderstood by purchasers, limiting their adoption despite delivering strong privacy outcomes for children.

The draft Code raises the following areas of concern:

- The extension of the Code to all online services that handles children's personal data, without sufficient clarity on thresholds such as "reasonably likely to be accessed by children" may make the Code unworkable.
- The requirement to assess and prioritise the "best interests of the child" without a defined decision framework, creating interpretive risk and inconsistency.
- Implicit expectations around consent in school-authorised or compulsory education contexts, where consent is often impractical or inappropriate.

In addition, the Code would benefit from greater clarity regarding the respective obligations (roles) of organisations that determine the purposes and means of processing children's personal information and those that process information solely on behalf of another organisation. Where a technology provider is contractually prohibited from using personal information for its own purposes and processes information solely to deliver a service requested by a school, many of the substantive decisions contemplated by the Code are in practice made by the school, not the provider. This lack of clarity creates practical uncertainty for schools and educational technology providers seeking to implement the Code.

At present, the draft does not provide sufficient certainty to begin full implementation planning and relies heavily on future OAIC interpretation and guidance, particularly around scope, roles (i.e., data controller vs processor), lawful basis and proportionality. We strongly recommend that the regulator consider overseas experience in implementing similar codes and ensure that these lessons and requests for clarity inform the development of the approach.

Distinguishing School-Directed EdTech from Consumer Digital Services

Parents cannot realistically assume responsibility for safeguarding decisions affecting millions of children in school communities.

Certain edtech services operate strictly within the institutional framework of a school. These services:

- are procured and controlled by schools, not accessed directly by children in a consumer context;
- are used solely to support the school's legal, administrative, and safeguarding functions;
- operate only on the instructions of the school, with no independent determination of purpose; and
- do not engage in profiling, advertising, or commercial exploitation of children's data.

Examples include platforms designed to support:

- media consent management,
- safeguarding recordkeeping,
- compliance with privacy and education obligations, and
- secure communication with parents and carers.

These services are best understood as institutional infrastructure to support accountability principle and duty of care; not standalone online services directed at children.

Applying the proposed Online Children's Code to such services would create unintended negative consequences:

Undermine Safeguarding Outcomes

Imposing requirements designed for consumer-facing platforms on compliance tools may:

- discourage school adoption,
- increase cost and complexity, and
- reduce consistency in consent and safeguarding practices.

Misalign Regulatory Burden

Where schools:

- determine the purpose of processing, and
- remain accountable for safeguarding obligations,

it is not appropriate to treat the service provider as an independent regulated digital service.

Reduce Availability of Purpose-Built Tools

Overly broad application of the Code risks disincentivising providers from offering:

- specialised compliance solutions,
- privacy-enhancing technologies, and

- tools that directly improve child safety outcomes.

Safeguarding for the Best Interests of the Child Should Include Collective Safety Outcomes

The best interests of the child should be assessed not only from the perspective of an individual student's privacy interests, but also in the context of the safety, welfare, and protection of all children affected by a school's safeguarding measures.

Where a technology demonstrably advances child safety, reduces risk, prevents harm, or enables schools to fulfil safeguarding responsibilities, regulators should recognise that the interests of children may be served by responsible use of the technology even where individual consent is not obtained.

This is particularly true where:

- The processing is necessary and proportionate (especially when compared with current alternative processes and their potential for failure);
- The technology serves a genuine safeguarding function;
- Less intrusive alternatives are not reasonably available;
- Strong governance and accountability measures are in place;
- Data is not used for advertising, profiling, or commercial exploitation.

In Schools, Duty of Care Must Take Precedence Over Consent

Schools owe a fundamental duty of care to every student in their care. This duty extends beyond education and encompasses student safety, wellbeing, protection from harm, and responsible management of school activities.

Many safeguarding technologies are used to assist schools in discharging these obligations. Examples may include technologies that:

- Manage student safety and security;
- Protect children from online harms;
- Ensure compliance with child protection requirements;
- Facilitate safe school communications;
- Support lawful safeguarding and welfare functions.

In these circumstances, the legal and ethical basis for processing should be necessity and duty of care rather than consent. A consent-based framework assumes that individuals can freely choose whether a particular processing activity occurs. However, safeguarding measures are fundamentally different from optional consumer services. For example, in the UK, if school processing is necessary to deliver education, protect children or meet statutory duties, it should not be based on consent. Consent is treated as appropriate only where the activity is genuinely optional and the purpose (and consequence) is narrow and simple to understand.

If a school determines that a technology is necessary to protect students, fulfil legal obligations, or safely administer educational activities, allowing voluntary individual opt-outs may compromise the effectiveness of the protective measure and create inconsistent outcomes across the student population. In some circumstances, obtaining consent may also place schools in an untenable position where they remain responsible for student welfare while being deprived of tools reasonably required to meet that responsibility. The result is a conflict between privacy compliance and child protection obligations.

The Code should avoid creating such conflicts.

We are concerned that an over-reliance on child or parental consent as a primary compliance mechanism in these contexts' risks undermining both the effectiveness and integrity of institutional safeguards. In school environments, where there are clear duties of care and accountability frameworks, shifting responsibility onto individual consent mechanisms can dilute organisational accountability, create inconsistency in protections, and introduce operational complexity that ultimately weakens, rather than strengthens, privacy outcomes. The Code should therefore avoid defaulting to consent where stronger, organisation-led protections are more appropriate, and instead reinforce aligned models of responsibility that preserve duty of care while maintaining high standards of data protection.

What similar overseas jurisdictions are doing: The UK ICO Approach

The UK Information Commissioner's Office (ICO) provides a well-developed and highly relevant framework for distinguishing between categories.

The ICO states that the Children's Code does not apply where an edtech provider:

- does not offer services on a direct-to-consumer basis;
- processes personal data only to fulfil the school's educational functions; and
- acts solely on the instructions of the school, without independent purposes.

In such circumstances, the edtech service is considered a "digital extension of the school's offline activities", with the school retaining control over the purposes and means of processing. This distinction ensures that regulation is risk-based and proportionate, targeting services that create genuine risks to children, while not impeding those that support institutional safeguarding responsibilities.

Edtech services designed to manage media consent, compliance and other safeguarding functions in schools clearly fall within this lower-risk category. These services:

Enable Legal and Safeguarding Obligations

Schools are required by law to:

- obtain and manage parental and student consent for media use,
- ensure appropriate use of student images and information, and
- maintain records demonstrating compliance with privacy and safeguarding requirements.

An edtech platform focused on safeguarding and compliance:

- does not introduce new data uses but enhances an existing function, but
- provides scalable, structured, auditable mechanisms to ensure these obligations are met.

Operate Under Institutional Control

- Access is restricted to school communities (staff, parents, carers, students where appropriate).
- The school determines what data is collected, how it is used, and when it is retained or deleted.
- The provider does not act independently or influence outcomes beyond implementing school instructions.

Do Not Present Code-Targeted Risks

These services do not:

- operate on a direct-to-consumer basis,
- use behavioural advertising or profiling,
- employ persuasive or addictive design patterns, or
- monetise children's attention or personal data.

Instead, they reduce risk and harm, enhance transparency, and strengthen accountability.

Our Code Recommendation: A School Safeguarding Technology Exception

Technologies deployed by or for educational institutions for the primary purpose of child safeguarding, welfare, duty of care, parental permission management, educational administration, or legal compliance should be subject to a modified compliance framework rather than the full requirements applicable to commercial consumer services.

We recommend that the Code include an explicit and narrowly tailored exemption permitting the use of educational and safeguarding technologies where:

1. The primary purpose is safeguarding, child protection, student welfare, safety, or the fulfilment of a school's duty-of-care obligations;
2. The processing is necessary, proportionate, and demonstrably in the best interests of the child;
3. The technology is used solely for educational, administrative, or safeguarding functions;
4. Appropriate privacy, security, retention, transparency, and accountability controls are implemented;
5. Personal information is not used for marketing, behavioural advertising, profiling, product development unrelated to the educational purpose, or other commercial purposes.

Under this approach, schools and educational technology providers would remain subject to robust privacy and accountability obligations while avoiding a consent-based framework that may unintentionally undermine child protection, welfare, and safeguarding outcomes. The Code should recognise that technologies deployed to protect children operate within a fundamentally different context from commercial consumer services and should therefore be assessed through a lens of necessity, proportionality, and the best interests of the child.

A number of high-profile incidents involving breaches in education technology have typically arisen in platforms characterised by large-scale data aggregation, broad functionality, and secondary commercial uses of children's information. In contrast, safeguarding tools are generally purpose-limited, operate under strict institutional control, and are designed to minimise data processing while identifying and mitigating risks to student wellbeing. Applying the same compliance model to both categories risks obscuring these critical differences and misdirecting regulatory effort away from the sources of greatest exposure.

More importantly, over-prescriptive requirements – particularly those that rely heavily on individual child or parental consent – risk undermining the effectiveness of safeguarding frameworks. In school environments, safeguarding is fundamentally grounded in institutional duty of care and accountability. Shifting responsibility onto fragmented consent mechanisms can weaken this model, introduce inconsistencies in protection, and create barriers to timely intervention. At worst, it may discourage schools from deploying, or vendors from developing, tools that are specifically designed to protect children from harm.

For these reasons, it is essential that the Code explicitly recognises safeguarding technologies as a distinct category requiring tailored treatment. A failure to do so risks creating a chilling effect on the development and adoption of privacy-enhancing, safety-critical tools, ultimately leaving children less protected in practice despite stronger formal regulation. A more precise, risk-aligned approach, one that distinguishes between data-intensive commercial platforms and tightly controlled safeguarding solutions, would better support both the protection of children's privacy and their broader safety and wellbeing.

Providing this clarity will:

- support schools in continuing to meet their safeguarding and compliance obligations,
- ensure children benefit from technologies that enhance their protection, and
- avoid unintended regulatory impacts that may reduce the availability or effectiveness of these tools.

Conclusion

In conclusion, we reiterate our strong support for the regulator's objective of embedding children's best interests at the centre of the digital ecosystem and for the important role this Code will play in raising standards across the market. However, for the Code to achieve its intended outcomes, it must be sufficiently precise to reflect the realities of how technologies are designed, deployed, and used in practice, particularly in institutional settings where duty of care and accountability frameworks already apply.

We therefore urge the regulator to explicitly recognise the distinction between data-intensive, commercially driven services and those designed to support compliance, which are purpose-limited, privacy-enhancing, and safety-focused. Where a school has determined – following an appropriate risk assessment – that a safeguarding measure is necessary, governance should appropriately rest with the school in discharge of its duty of care, rather than being contingent on individual consent preferences.

We recommend that the Code include clear guidance on the respective responsibilities of organisations that determine the purposes and means of processing children's information and organisations that process information solely on behalf of those entities. This would assist schools and technology providers in implementing the Code consistently and effectively while ensuring accountability remains appropriately allocated.

Such distinctions should be reflected in the Code through clear scoping, proportionate application, or defined pathways, to ensure that safeguarding and low-risk edtech solutions are not subject to disproportionate or counterproductive requirements. Care should be taken to avoid over-reliance on individual consent mechanisms in contexts where organisational accountability is both more appropriate and more effective.

A Code that differentiates in this way will not dilute protections – it will strengthen them by directing regulatory effort where risks are greatest, while supporting the continued development and adoption of technologies that demonstrably enhance children's privacy and safety. We would welcome continued engagement with the regulator to help ensure the framework strikes this balance in a way that is both practical and durable.