EduGowth Limited
ABN: 42 612 800 594

Melbourne, Australia
edugrowth.org.au

Office of the Australian Privacy Commissioner
via copc@oaic.gov.au

Submission - Children's Online Privacy Code

Introduction

EduGrowth welcomes the opportunity to contribute to the development of the Children's Online Privacy Code (Code).

As Australia's education technology and innovation industry hub, EduGrowth represents a national network of EdTech companies, education providers, researchers and institutions committed to building a globally competitive, learner-centred EdTech ecosystem supporting education in the digital age.

The proposed Code represents a significant and timely opportunity to uplift privacy standards for children in digital environments. We strongly support the intention to place children's rights at the centre of online privacy protections and to ensure those protections are both meaningful and actionable.

Our submission reflects insights gathered from our members, sector consultations, and direct engagement with the Office of the Australian Information Commissioner (OAIC).

A well-designed Children's Online Privacy Code has the potential to:

- Lift privacy standards across the sector while providing clarity and guidance tailored to EdTech providers;
- Create national consistency to reduce fragmentation and compliance complexity;
- Applies equitably to both domestic and international platforms;
- Recognises lawful data retention obligations specific to education settings;
- Supports innovation through scalable compliance models for StartUps and ScaleUps;
- Provides practical guidance on layered consent in school environments; and
- Refines the Designated Internet Services category to treat institutional EdTech distinctly from general-purpose platforms.

Summary of Key Positions

Opportunities for the Code

- The Code can provide a clear framework for EdTech companies to design with child privacy in mind
- The Code has the opportunity to establish a consistent national approach across states and territories, reducing ambiguity and improving implementation within the education sector
- The Code could promote sector-wide improvement in child data governance and encourage privacy-by-design practices that align with, or set, international best practice
- The Code could establish clear expectations for responsible EdTech use in schools, while building confidence develop and deploy innovative tools

Concerns about the Code

- The Code must not adopt a one-size-fits-all model that imposes equal obligations on fundamentally different types of digital services
- EdTech providers operating within regulated school environments must be distinguished from freemium ad-driven platforms
- Without targeted guidance, smaller providers and StartUps may face disproportionate compliance burdens, potentially stifling innovation and limiting schools' access to privacy-conscious Australian solutions

Clarifications about the Code

- Further clarity is required around the application of consent in educational contexts, particularly regarding the role of school leaders, parents, and education authorities in providing or authorising consent on behalf of children
- The intersection between the Code and existing education laws and policies needs to be carefully mapped to avoid duplication or conflict, especially where privacy obligations already exist through departmental policies or state adopted regulation
- Education is a unique use-case in relation to the "right to be forgotten" - students, or their guardians, may not have the authority to delete educational records such as assessment results, attendance data, or enrolment history, which are often governed by statutory retention schedules, regulatory oversight, or accreditation obligations

Summary of Recommendations

1. Frame the Code as a nationally harmonised privacy standard mandated across all states and territories.
2. Develop and release sector-specific implementation guidance with checklists and examples relevant to EdTech, schools, and institutional settings.
3. Apply the Code's requirements equally to Australian and international providers to ensure fair and competitive market conditions.
4. Clarify how the Code accommodates legitimate data retention obligations under educational and operational requirements.
5. Consider a staged or scalable compliance model for emerging and small providers, consistent with the proportionality principles already embedded in the APP framework.
6. Provide guidance on how the Code interacts with institutional consent frameworks.
7. Embed proportionality into the Code by tailoring obligations based on function, risk profile, and operating environment.

Recommendations

Ensure National Consistency

EdTech providers often face differing privacy interpretations and implementation practices across states and territories. This fragmentation creates complexity for companies operating nationally, increases compliance costs, and can result in inconsistent protections for children.

A well-designed Code has the potential to harmonise privacy expectations and processes across jurisdictions — benefiting schools, families, and providers alike. To realise this benefit, States and Territories should be actively engaged in the Code's development and encouraged to adopt it as the definitive standard, rather than treating it as a minimum baseline upon which to layer additional, jurisdiction-specific requirements.

Without such alignment, there is a risk that the Code will add yet another layer to an already complex regulatory environment — particularly for EdTech companies serving schools across multiple jurisdictions.

Recommendation - 1

relates to Questions 1.3

Frame the Code as a nationally harmonised privacy standard mandated across all states and territories.

Publish Plain English Guidance for Providers

The Code's success will depend not only on what it requires, but on how clearly those requirements are understood and implemented by the wide range of APP entities it applies to.

Many EdTech providers, particularly StartUps, ScaleUps, and smaller education service platforms, do not have the resources to engage external legal counsel and often face challenges interpreting legal or regulatory documentation.

To ensure meaningful compliance and encourage early adoption, the Code should be supported by plain-language, and sector-specific guidance. This should include:

- Clear definitions of expectations
- Worked examples of how obligations apply in education settings
- Checklists and decision tools tailored to EdTech use cases; and
- Guidance suitable for both technical teams and education leaders procuring these tools

By making the Code more accessible, such guidance would reduce compliance ambiguity, uplift overall privacy literacy, and ensure that well-intentioned providers are not penalised simply for lack of regulatory clarity. It would also help align implementation across sectors and jurisdictions by promoting a shared understanding of key obligations.

Recommentation - 2

relates to Questions 4.1, 4.4, 5.1, 5.4

Develop and release sector-specific implementation guidance with checklists and examples relevant to EdTech, schools, and institutional settings.

Create a Level Playing Field for Australian Providers

To foster innovation and ensure fair market conditions, the Code must apply equally to both domestic and international EdTech platforms that collect and use personal information about Australian children.

Many global technology companies operate at scale in Australia, often with greater legal, compliance, and financial capacity than domestic providers. If international platforms are not held to the same standards under the Code - whether due to enforcement challenges, jurisdictional limitations, or lack of regulatory clarity - it risks creating a two-tiered system. One where Australian companies bear the full cost and compliance responsibility, while offshore providers leverage market dominance and have the financial means to challenge enforcement through lengthy legal processes or factor possible fines into their business model.

This disparity is particularly evident in school procurement, where compliance with privacy standards is an increasingly important factor in platform selection. Without consistent application, the Code may unintentionally disadvantage privacy-conscious Australian EdTech companies competing in the same ecosystem.

A level playing field is not only a matter of commercial fairness — it is essential to building a credible, enforceable privacy regime that protects all Australian children equally, regardless of which service they use or where that provider is based.

Recommentation - 3

relates to Questions 2.1, 2.3, 2.5

Apply the Code's requirements equally to Australian and international providers to ensure fair and competitive market conditions.

Recognise Lawful Data Retention Obligations in Education

In educational settings, there are often legitimate and legally mandated reasons to retain a student's personal information beyond their active use of a digital platform. These include compliance with state and federal education laws, school registration and reporting requirements, certification and accreditation processes, and audit obligations tied to public funding or assessment frameworks.

Unlike commercial platforms where data deletion is often a consumer right, education data is sometimes not subject to individual discretion, students, or even their guardians, may not have the authority to delete test results, attendance records, or academic progress reports. EdTech providers operating in these environments are often required to maintain data securely, even after a child is no longer an active user.

If the Code does not clearly recognise these lawful retention requirements, EdTech providers may be forced to choose between breaching privacy obligations or failing to meet education compliance expectations. This could create significant operational and legal uncertainty for both providers and schools.

Recommentation - 4

relates to Questions 13.3, 13.4

Clarify how the Code accommodates legitimate data retention obligations under educational and operational requirements.

Support Innovation Through Proportional Compliance

Australia's EdTech StartUps and ScaleUps play a vital role in driving innovation, improving educational access, and responding rapidly to emerging learner and system needs. However, these early-stage companies often face significant resource constraints and operate without the legal or compliance infrastructure available to more mature firms.

The cost of establishing, maintaining, and demonstrating full-scale privacy frameworks, especially in alignment with new regulatory obligations, can be a material barrier to entry for smaller providers.

Without consideration of their capacity, the Code risks inadvertently skewing the market in favour of larger incumbents, discouraging experimentation and investment in locally developed, privacy-conscious solutions.

Importantly, the principle of proportionality is already embedded in the Australian Privacy Principles (APPs), which allow for context-specific and risk-based implementation. The Code should build on this existing foundation and apply it clearly and explicitly to early-stage EdTech providers.

Such an approach would not weaken the Code's protections — rather, it would ensure that innovation and privacy can coexist by enabling responsible providers to grow into compliance as they scale.

Recommentation - 5

relates to Questions 2.6, 2.7

Consider a staged or scalable compliance model for emerging and small providers, consistent with the proportionality principles already embedded in the APP framework. Include simplified obligations, transitional pathways, and access to shared privacy tools to support early-stage compliance.

Address the Complexity of Consent in School Environments

The Code must recognise that consent in educational settings operates differently from general consumer platforms. EdTech providers working with schools typically operate within institutional consent frameworks governed by education legislation, departmental policies, and procurement contracts. These frameworks involve layered authorisation, where responsibilities are shared between education departments, school leaders, parents or guardians, and students themselves when they have the capacity to provide that consent.

While the Code rightly emphasises the importance of empowering children, it must also account for legal and operational realities. In many cases, school-based use of EdTech services is authorised by the institution on behalf of the student, particularly for curriculum-aligned or department-mandated tools. Treating children as individual consumers in these contexts could create unnecessary regulatory conflict, duplicate consent processes, or undermine school duty-of-care obligations.

Moreover, the notion of "developmentally appropriate consent" must be aligned with the realities of how education is delivered and take into account times where consent is not optional such as for mandated assessments or compliance reporting.

To assist with implementation and avoid confusion, the Code should provide clear guidance and example scenarios that illustrate how consent applies across typical school settings, year levels, and service types. It should also direct guidance to both EdTech providers and school-based decision-makers, ensuring shared understanding of responsibilities and reducing the risk of inconsistent application.

Recommentation - 6

relates to Questions 3.1, 6.4, 6.5, 9.1, 14.3, 15.3

Provide guidance on how the Code interacts with institutional consent frameworks

- Include example scenarios to illustrate appropriate consent handling within schools
- Reinforce the role of adult responsibility and institutional safeguards over sole reliance on child consent
- Guidance should be directed at both EdTech providers and school-based decision-makers, ensuring shared understanding and consistent implementation

---

Prioritise Context-Sensitive Regulation

The Code must account for the wide diversity of services captured under the Designated Internet Services (DIS) category; which, as defined in the Online Safety Act, includes any online service that allows users to access or receive material over the internet. This broad classification rightly includes EdTech platforms, but to ensure proportional and effective regulation, the Code should formally recognise EdTech as a distinct subcategory within DIS.

EdTech platforms, particularly those used in formal school settings under institutional duty of care differ significantly from other DIS platforms in terms of purpose, data risk, governance, and deployment context. Unlike general internet services, EdTech tools are typically selected through government or school procurement processes, subject to education legislation, and used in supervised environments.

This refinement would not dilute protections, it would enhance clarity, improve enforceability, and ensure obligations are aligned with real-world risk.

Recommentation - 7

relates to Questions 1.1, 2.6, 2.7

Embed proportionality into the Code by tailoring obligations based on function, risk profile, and operating environment.

About EduGrowth

EduGrowth is Australia's education technology and innovation industry hub. Through connection and collaboration we accelerate Australia's EdTech ecosystem globally.

We are connecting a community of education providers, industry participants and EdTech entrepreneurs committed to reimagining learning in the digital age. As education transitions to borderless digital delivery, our diverse ecosystem will impact the future of learning globally from Australia.

Our programs focus on developing the entire education technology and innovation sector. We have a range of services supporting EdTech companies at each stage of their journey, whilst also connecting education providers and industry participants into the broader ecosystem.

We'd welcome the opportunity to discuss this in greater detail, please contact

[redacted]