28th May 2026

Ms Carly Kind
Australian Privacy Commissioner
Office of the Australian Information Commissioner

by email: copc@oaic.gov.au

Response to the OAIC Exposure Draft on the Children's Online Privacy Code 2026

Qoria is pleased to provide this submission with respect to the Children's Online Privacy Code 2026 Exposure Draft.

We are an Australian based and ASX listed, global online safety technology company dedicated to supporting digital safety in homes and schools through a connected ecosystem. Through our services, supporting more than 30,000 schools and 9 million parents to protect 30 million children we have a unique perspective on what works.

Privacy, safety and the interests of children

In recent times, we've seen policy makers and regulators responding to concerns about the safety, security, rights of parents, rights of students and the potential for misuse of technology in education. This is particularly so in the US where a stream of new laws are being proposed and passed.

Whilst perspectives on proper practices do differ markedly we find that all stakeholders and advocates in these debates have the good intentions of protecting and supporting children.

As a provider of student safety and wellbeing technology, we find our products sit in the middle of these dynamics.

Safety technology feature sets are frequently at the junction of competing stakeholder interests. For example, how do we reconcile a child's right to agency and privacy against school duty of care and parental rights or requests for visibility?

Our platform seeks to bring together schools, students and their parent communities, matters of sharing, security, consent, bias, agency and so on are fundamental.

We are thus uniquely positioned to assess the effectiveness of global regulatory interventions.

What we seek to communicate in this submission is this.

1. *Regulations need to empower guardians, because engaged parents deliver better outcomes*
2. *Regulatory requirements need to be practically* **implementable** *and so broader regulatory work is required to force big-tech (operating systems and platforms) to open up their safety features so that more privacy-preserving and surgical safety/monitoring capabilities can be implemented.*

Regulations relating to the protection of children must respect the rights of parents and schools and empower them as their trusted guardians. Research clearly and consistently shows empowered parents are engaged parents and deliver better outcomes for children.

Regulations which can't be reliably implemented can be detrimental to their objectives. We believe we are seeing this play out in the Social Media ban implemented in Australia last year.

And regulations seeking to protect children must be anchored in a fulsome appreciation of child wellbeing. An absolutist and narrow focus, for example on privacy, is extremely likely to abandon a child in a private space and in the face of digitally sourced harm.

Ultimately privacy and safety are not opposite sides of a coin. They are deeply interrelated in society's mission to deliver what's in the best interests of a child and all children.

Our detailed submission follows. It sets out our position on scope and platform interoperability, the "strictly necessary" default, the best interests of the child, consent, monitoring notification, the right to destruction, privacy impact assessments, age assurance and the transition period, together with our specific recommendations.

Managing Director, Qoria

Review and recommendations

1. Scope: proportionate treatment of edtech and the case for platform interoperability

This is the most significant issue for Qoria. The Exposure Draft applies the Code to school-directed edtech services on the same footing as consumer-facing platforms, and the Explanatory Statement to Section 5 expressly cites "online school management systems that monitor student performance" as in-scope. We submit that school-directed edtech presents a different risk profile and warrants a proportionate approach. We also urge the OAIC to address a structural barrier that limits how well safety tech can protect children: the closed nature of major consumer platforms.

1.1 The school as trusted intermediary

Where an edtech service is deployed by a school, the school is the trusted intermediary between provider and child. The school selects, procures and configures the service, and determines the purposes for which children's data is used. The provider acts solely on the school's instructions and does not use children's data beyond those instructions. This is fundamentally different from consumer platforms, where the provider sets the purposes and engages directly with the child.

1.2 Existing safeguards

Australian schools are already subject to extensive obligations under State and Territory education law, child safety frameworks and (for government schools) the APPs themselves. Edtech providers are bound by school procurement contracts that routinely cover data handling, security, retention and deletion. Layering the full weight of the Code on top of these arrangements creates duplication without measurable benefit for children.

1.3 International precedent

The UK ICO's Age Appropriate Design Code recognises that services provided in a school context, where the provider processes data solely on the school's instructions, may sit outside its scope. We urge the OAIC to take a similar approach.

1.4 Proposed approach

We propose the Code exclude, or apply a lighter-touch regime to, edtech services where all of the following apply:

- the service is not accessed on a direct-to-consumer basis;
- the provider only processes children's data to fulfil the school's educational and child safety purposes, on the school's instructions; and
- the provider does not process children's data for any other purpose (including its own marketing, product development or commercial analytics).

This protects children, recognises the existing governance of the school sector, and avoids compliance costs that would ultimately reduce the availability and affordability of safety technology for schools and families.

1.5 The need for platform interoperability

Big tech gets in the way of privacy respecting safety

Regulators need to appreciate that the most well meaning platform providers (e.g. social, gaming, education or safety) are often fundamentally limited in what they can practically provide in terms of balancing customer requested capability with privacy.

This is particularly stark in online safety where big tech platforms place technically unnecessary impediments in the way of privacy preserving approaches.

Examples include:

- Google does not provide standardised approaches to monitor user activity on Google devices such as Android tablets or Chromebooks. Safety technology providers use what is effectively a hack of the "Accessibility protocols" of these platforms to scrap activity and limit malfeasance.
- Apple does not permit consumer safety app developers to access their vast, powerful and secure Device Management capabilities despite offering this to enterprise developers.
- Apple does not provide standardised approaches for safety apps to access content in Apple platforms eg in iMessage. Consequently safety apps use what is effectively a hack by downloading back-ups for scanning. This is less than ideal.
- Apple does not permit schools to auto-install certain safety capabilities on devices such as key-log or audio capture. Apple requires end-users (i.e. students) approve them and permits them to disable them. Consequently school safety providers often use less privacy preserving approaches to deliver duty-of-care such as scanning student cloud accounts.
- End-to-end encrypted messaging platforms, including those operated by major social media companies, provide no privacy-preserving signal to safety providers about content concerns (for example, indicators of grooming, self-harm or coercion), forcing schools and safety providers to rely on broader device-level monitoring than would otherwise be necessary.

These limitations are not technical. They are commercially driven by big tech and result in a blunt approach to data collection for the purpose of harm prevention and intervention.

We strongly urge the Commissioner to work with other agencies, including the ACCC and eSafety to demand interoperability of safety features. The capability to provide privacy preserving, surgical approaches to safety largely exists. These groups need to be brought to the table and forced to establish a standards based, interoperable and open-access environment for privacy and safety.

Recommendations

1. A cross government approach to regulation is necessary to ensure that key (gate-keeper) technology platforms provide open, interoperable access to their safety and security capabilities in order to support capability and competition in online safety technology. Such regulatory work includes privacy, safety and competition law.

2. As an interim, privacy-positive step, the OAIC should expressly recognise on-device, school-deployed safety technology as an acceptable means of age assurance and age-appropriate experience under the Code, so that children's personal information does not need to be handed to dominant platforms in order to enforce age-appropriate settings.

2. “Strictly necessary” default (Section 9)

We support high privacy by default; however, limiting data collection to situations that are “strictly necessary” and in the context of a “specific child” is a standard which we believe will lead to children being unnecessarily harmed.

Our explanations for this conclusion are set out in subsequent sections; however, schools must monitor student activity as part of their duty of care. In doing so, data will be captured which may not be strictly necessary with respect to a particular child but will be necessary to protect the cohort of students.

A workable application of "strictly necessary" must turn on the primary purpose of the service as procured. Where a school engages a provider to deliver online filtering, monitoring or other safeguarding functions, the safeguarding purpose is the primary purpose. The data collection required to deliver that purpose, including content inspection, activity logging and signal analysis across the student cohort, is strictly necessary to the service, even where that collection is extensive. Treating safeguarding data as ancillary, or as a feature that must be switched off by default, would defeat the very purpose for which the school selected and deployed the service in the first place. The "strictly necessary" test should therefore be applied to the service-as-deployed and to its stated primary purpose, not to a hypothetical minimal service stripped of the protections the school has expressly procured.

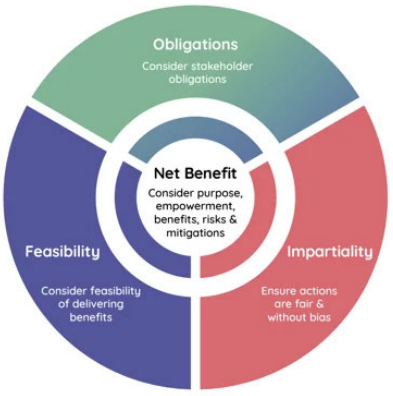
In our view the best interests of the child are best served by respecting the role and capability of schools to manage this balance. In fact we organise our entire company around this idea through the Qoria **ethical framework**.

Our framework requires that when considering the use of technology that we and our school clients ensure that:

1. legal obligations can be adhered to;
2. actions can be taken without bias to any user or group;
3. technology is reliable and fit for purpose;

and after all that, ensure that:

4. there is a **positive net benefit** to the use of the technology after considering risks, benefits and mitigations.



Education settings are different

The Exposure Draft seeks to apply the Code to school-directed edtech services on the same basis as consumer-facing platforms. The Explanatory Statement to Section 5 expressly states that “online school management systems that monitor student performance” are in-scope.

Applied to school-directed edtech without adjustment, the Code will create four operational problems that, in our view, will reduce rather than improve outcomes for children:

1. **Consent:** in a school deployment, the lawful basis for processing is the school’s educational and safeguarding purpose, mediated through parental acknowledgement at enrolment. Treating individual student consent as the operative mechanism, particularly for safety monitoring, would undermine the school’s ability to discharge its duty of care.

2. **Right to destruction:** schools are required by State and Territory education law to retain student welfare and safeguarding records, often for many years after the student leaves. A direct-to-provider destruction right cuts across these retention duties and may also remove evidence relevant to ongoing safeguarding matters. The right must operate through the school as a data controller.

3. **Privacy impact assessments:** most Australian schools do not have in-house privacy capability to assess each edtech service individually. In the United States, this gap is filled by recognised third-party frameworks (for example, the Student Data Privacy Consortium's National Data Privacy Agreement and iKeepSafe certifications), which allow a single provider assessment to satisfy thousands of schools. The Code should permit a single provider PIA, supplemented by school-specific deployment notes, rather than a separate PIA per customer.

4. **"Strictly necessary":** school safeguarding is inherently a cohort-level activity. To identify a child at risk of self-harm, grooming or violence, a monitoring service must process activity data across the whole student body, most of whom are not at risk on any given day. Tested against a single child in isolation, that collection is not strictly necessary; tested against the cohort, it is essential. The Code needs to accommodate this cohort-level safeguarding logic, otherwise it will inadvertently prevent the very protections it is intended to support.

The UK ICO's Age Appropriate Design Code recognises that services provided in a school context, where the provider processes data solely on the school's instructions, may sit outside its scope. We urge the OAIC to take a similar approach.

Recommendations

1. Carve out, or apply a lighter-touch regime to, school-directed edtech services where the provider acts solely on the school's instructions for educational or child safety purposes and does not process children's personal information for its own commercial purposes. This aligns with the approach taken by the UK ICO under the Age Appropriate Design Code.

2. Where school-directed services remain within scope, the Code should expressly recognise school-mediated consent and acknowledgement, a single provider PIA covering the service as deployed, and the school as the appropriate recipient of access, correction and destruction requests in respect of school-instructed processing.

3. Amend Section 9 (or, alternatively, addressed in OAIC guidance) so that the "strictly necessary" test is applied by reference to the primary purpose of the service as procured and to the core service the child, parent or school has signed up for. Where a feature forms part of the core service, including safeguarding functions such as online filtering and monitoring procured by a school, the personal information required to deliver that feature should be treated as strictly necessary, even where collection is extensive. This preserves the protective intent of the "strictly necessary" threshold against secondary or commercial uses, while ensuring that the Code does not inadvertently disable the very services schools and parents have chosen to keep children safe.

4. Reframe Section 9 (or address in OAIC guidance) so that the "strictly necessary" test is assessed against the service as procured by the person responsible for sign-up, whether that person is the child, a person with parental responsibility or a school acting in the place of a parent. This is necessary because in a significant set of services within the Code's scope (parental controls, early childhood development trackers, family photo sharing applications, internet-connected baby monitors and school-issued device management) the data subject is not the party who signs up, and the OAIC's current framing cannot be coherently applied to them.

A drafting issue: data subject is not always the person who signed up. The Explanatory Statement to Section 9 anchors the "strictly necessary" test to "the elements of the service the child has signed up for". In a consumer context this makes sense. In a significant set of services within the Code's scope, it does not. In parental control products, the parent installs and configures the service; the child is the data subject but has not signed up for anything. The same structural mismatch arises in early childhood

development trackers, family photo sharing applications, internet-connected monitors and school-issued device management programmes, all of which the OAIC has expressly brought into scope under Section 5. Read literally, the OAIC's own framing would treat almost everything these services do as not strictly necessary, because the data subject is not the party whose sign-up defines the service.

A workable test: primary purpose and the person responsible for sign-up. We respectfully suggest the test be reframed so that "strictly necessary" is assessed against the primary purpose of the service as procured by the person responsible for sign-up, whether that person is the child, a parent or a school acting in place of the parent, and against the elements of that service as defined at the point of procurement. Where a school engages a provider to deliver online filtering, monitoring or other safeguarding functions, the safeguarding purpose is the primary purpose of the service. The data collection required to deliver that purpose, including content inspection, activity logging and signal analysis across the student cohort, is strictly necessary to the service, even where that collection is extensive. The same logic applies to parental control deployments and the other Section 5 services in which the data subject is not the procurer.

This reframing preserves the protective intent of the "strictly necessary" standard against secondary and commercial uses such as direct marketing, behavioural advertising, generalised service improvement, AI model training on children's personal information and any indirect funding model that monetises children's data. Each consideration above is offered to help the OAIC arrive at a test that is internally consistent across the categories of service it has chosen to bring within scope.

3. Best interests of the child (Sections 10 and 11)

We strongly support the best-interests principle, which aligns naturally with our products' design intent. Where a school has assessed a service as being in students' best interests through its own procurement and safeguarding processes, that assessment should be a relevant and weighty factor in the provider's own evaluation: schools owe a duty of care to their students and are well placed to make this assessment in context. We encourage the OAIC to publish guidance on how the best-interests assessment should be documented and applied, particularly in school-directed contexts, to support consistency across the sector.

4. Consent and the role of schools (Sections 12 to 21)

The Code sets consent at 15, above the UK AADC's 13. In school-directed deployments, parental consent or acknowledgement is typically obtained at enrolment and device deployment, so the practical impact is less acute than for consumer services. We would welcome confirmation of whether the threshold is intended to apply uniformly or whether differentiation is possible based on risk and governance context.

Three further points warrant clarification. First, the Code should explicitly recognise school-mediated consent or acknowledgement as a valid mechanism under Section 13(2): schools already verify parents and guardians at enrolment, and a separate verification step would add friction without strengthening protection. Second, on assent (Section 20), the OAIC should clarify how the requirement applies where settings are pre-configured by the school or parent before the child uses the device. Third, on the 12-month expiry (Section 15(4)), annual consent renewal aligns naturally with the school enrolment cycle, and the OAIC should confirm that consent obtained at annual enrolment satisfies the currency requirement.

5. Monitoring notification (Section 33)

Section 33 is directly relevant to our core products and we support the underlying transparency principle. We propose that compliance can be met through an age-appropriate notice presented when the child first uses a device on which our software is active, with the notice remaining easily accessible thereafter. As monitoring is configured by the school's IT team before the device reaches the child, "as soon as practicable" should be interpreted as the point at which the child first uses the device, not the point of configuration. Schools also already inform students about monitoring through acceptable use policies, digital citizenship and pastoral care; where they have done so, this should be a relevant factor in assessing compliance.

6. Right to destruction (Section 32)

We support the principle, which aligns with children's rights under the UNCRC. In school-directed deployments, the school determines purposes and means and the provider acts on instructions; destruction requests in respect of school-held data should therefore be directed to the school, which then instructs the provider. This avoids destruction of records the school may be required to retain under education legislation. Granular, verifiable deletion across all storage locations is a significant technical undertaking and we ask the OAIC to factor this into the transition period.

7. Privacy impact assessments and public register (Sections 38 and 39)

For school-directed edtech, a single PIA covering the service as deployed should suffice, rather than a separate PIA for each school: data flows and privacy impacts are materially the same, and per-school PIAs add cost without additional benefit for children. On publication, full PIAs risk exposing commercially sensitive product, security and architecture detail. The public register should list the name, date and scope of each PIA, with the full assessment available to the Commissioner on request, balancing transparency with legitimate commercial interests.

8. Age assurance (Section 8)

Section 8(5) allows an entity to avoid age assurance entirely if the Code's protections are applied to all end-users. For school-directed services, where users are known to be children via the school's student information system, this is the most practical path.

On platform-level age gating more broadly, we reiterate the concerns set out in our Issues Paper response: high cost, the privacy risks of collecting personal data to prove age, ease of avoidance via VPNs and location spoofing, weak enforcement against offshore services, and high error rates.

This is clearly Australia's experience since the social media bans and introduction of pornography website age-gating requirements.

Recommendations

1. Confirm in guidance that, where users of a service are known to be children through a verified source (such as a school's student information system), no further age assurance is required, provided the Code's protections are applied uniformly to all end-users.

2. Recognise on-device safety technology, capable of communicating age tokens or policy signals to platforms without sharing the child's personal information, as a privacy-preserving age-assurance method, and treat any centralised age-verification approach as a measure of last resort.

9. Transition period and commencement

We advocate for a transition period of at least 12 months from registration. This is required because:

- school-directed providers must coordinate compliance across thousands of school customers, each with its own governance and procurement;
- school procurement and contracting cycles are annual, so changes to data handling, consent and policies can only land at natural renewal points;
- technical changes (granular deletion, high-privacy defaults, child-friendly notifications) require significant development, testing and deployment;
- PIAs must be completed, reviewed and registered before changed services are released; and
- staff training must be developed and delivered to all personnel with regular access to children's data.

We ask the OAIC to publish clear milestones and a phased timeline, allowing entities to prioritise the most critical compliance steps (high privacy by default, best-interests assessment) while permitting more time for complex operational changes.

10. Closing

Qoria is committed to children's safety and privacy online and supports the OAIC's objectives. We urge the OAIC to recognise the distinct role and risk profile of school-directed edtech, to address the structural role of dominant platforms through interoperability obligations, and to apply the Code's requirements proportionately.

We welcomed the opportunity to participate in the OAIC's roundtables and look forward to further consultations.