Submission to the Office of the Australian Information Commissioner

Re: Exposure Draft - Privacy (Children's Online Privacy) Code 2026
Submitted by: [redacted] Co-Founder Ablative Pty Ltd
ABN: ABN pending- company in formation
Contact: [redacted]
Phone: [redacted]
Date of submission: 1/06/2026
Submitted via email to copc@oaic.gov.au

EXECUTIVE SUMMARY

We support the Code. We want it to be strong, clear, and workable. Our submission offers seven positions informed by the practical reality of designing a system that handles children's sensitive information in an educational setting:

1. Educational technology that processes children's sensitive data should be unambiguously within scope and we welcome **Section 5's** inclusion of these services.

2. The "strictly necessary" standard in **Section 9** is the right threshold for children's data, but the Code would benefit from recognising that some services collect data about children rather than from them, and this distinction matters for how the standard is applied.

3. The consent framework in Division 2 is comprehensive, but needs careful thought around educational contexts where consent involves schools, parents, and children simultaneously.

4. The best interests principle in **Sections 10 and 11** should explicitly account for children with disability, neurodivergence, and developmental differences, not as an afterthought, but as a design requirement.

5. The right to request information about automated decision-making in **Section 28(2)(g)** is welcome, and we urge the OAIC to provide guidance on what constitutes meaningful disclosure for systems that generate inferences about children without making decisions about them.

6. The destruction right in **Section 32** is appropriate, but the Code should address how it interacts with observation-based data where multiple data subjects may be involved.

7. Privacy impact assessments under **Section 38** should be required to specifically address the risk of harm from mislabelling, deficit framing, and inappropriate categorisation of children, not only from data breaches or unauthorised access.

SPECIFIC RESPONSES TO THE EXPOSURE DRAFT

Part 2 - Application of this Code

Section 5: Additional entities bound by this Code

We strongly support the inclusion of services "primarily concerned with the activities of children" even where the child is not the direct end-user. This captures a category of services that handle some of the most sensitive information about children but would otherwise fall through gaps in the Code's coverage. Note 1's examples - applications that track early childhood development, online

school management systems that monitor student performance - describe exactly the kind of service we are building. We welcome this clarity.

However, we want to flag one area where further guidance would help. Our primary users will be teachers and parents. Children interact with the platform in limited, supported ways- for instance, contributing voice reflections or self-assessments under teacher guidance. The child is both an indirect subject (observed by adults) and, in some modes, a direct participant. We believe this kind of service should be covered by the Code regardless of whether the child is classified as an "end-user" in the traditional sense. The Explanatory Statement's discussion of Section 5 supports this reading, and we would welcome an explicit statement to that effect in any guidance material.

We also note the health service exclusion in **Section 5(c)**. We will collect wellbeing data that could, in some readings, be characterised as health information under the Privacy Act. We want to be clear: we do not seek to use this exclusion to avoid the Code's obligations. An educational tool that collects wellbeing data about children should be held to the same standard as any other service handling children's sensitive information, regardless of how that data is classified. We would welcome clarification that the health service exclusion is not available as a loophole for EdTech platforms that happen to touch on wellbeing.

Part 3, Division 1 - General Requirements

Section 8: Ascertaining the age of end-users

The risk-based approach to age assurance is sensible. For services like ours, where children access the platform through school-managed accounts set up by administrators and parents, age is established through the enrolment process rather than through age verification technology. This is a legitimate and privacy-preserving approach - the school already knows the child's age, and requiring additional age verification would mean collecting more sensitive information to solve a problem that doesn't exist in this context. We support the Explanatory Statement's recognition that entities should consider "the suite of age assurance methods available, their relative efficacy, costs associated with their implementation, and data and privacy implications on end-users." For school-managed educational tools, trusted-context verification through the institutional relationship is the most proportionate and least privacy-invasive approach.

We do want to raise a practical concern. The obligation to destroy sensitive information collected for age ascertainment "as soon as practicable" under **Section 8(4)** is appropriate for consumer-facing services, but may interact oddly with educational contexts where the child's age is part of their ongoing educational record rather than a standalone data point collected solely for compliance purposes.

Section 9: Entities may collect etc. personal information about a child by default only if strictly necessary.

We support the "strictly necessary" standard. It is a higher bar than the existing "reasonably necessary" threshold, and rightly so. Children's data deserves that higher bar. For us, the practical implication is this: the observations that teachers and parents record about children- what they see, what they notice, what concerns or delights them- are strictly necessary for the service to function. Without observations, the platform has nothing to work with. The inferences the system generates from those observations (identifying relevant developmental dynamics, suggesting follow-up questions, recommending evidence-based support strategies) are also strictly necessary - they are the core service, not an add-on. What would not be strictly necessary: using children's data for advertising, for training models that will be sold separately, for product improvement beyond

what is needed to maintain the core service, or for any purpose unrelated to that specific child's educational support. The distinction matters because Section 9 is about default settings and system design, not about individual consent decisions. We read this as requiring that the system be architected so that, out of the box, it collects and processes only what is essential. Additional collection that serves the entity's broader interests rather than the child's educational needs should require an active, informed opt-in, and we agree with that approach.

Section 10: Collection consistent with best interests of the child

We support the best interests principle and its grounding in Article 3 of the UNCRC. We want to make two specific points. First, the Explanatory Statement's list of factors for assessing best interests includes, at item (f), consideration of whether "particular groups of children may experience disproportionate or adverse impacts (including children with disabilities, Aboriginal and Torres Strait Islander children, children from culturally and linguistically diverse backgrounds)." We would urge that this consideration be given greater prominence in any guidance material. For a platform like the one we are developing, which is specifically designed for use with neurodivergent children at its core, the question of whether data collection and use is in the best interests of a child with autism, ADHD, or an intellectual disability is not an edge case, it is the central design question. The best interests assessment must account for the fact that some data practices that are benign for neurotypical children may be harmful for neurodivergent children, and vice versa.

Second, we want to draw attention to a form of harm that the Code's best interests framework should explicitly recognise: the harm of deficit framing. A system that collects observations about children and generates inferences can easily default to cataloguing what is "wrong" with a child - their difficulties, their deficits, their deviations from a norm. This is not in the child's best interests even if every individual data point is accurately collected and securely stored. We are designing our system around positive language framing precisely because of this risk. The Code's best interests assessment should require entities to consider not just whether they collect data lawfully, but whether the way they frame and present inferences about children is consistent with the child's dignity and developmental wellbeing.

Section 11: Use or disclosure consistent with best interests

We support the requirement that both consent and best interests must be satisfied before an entity can use or disclose personal information about a child under APP 6.1. This dual requirement is important - consent alone is not sufficient if the use is not in the child's interests. For educational contexts, we want to highlight a specific scenario. When a teacher records an observation about a child, and our system generates inferences about relevant developmental dynamics, those inferences are a form of "use" of the child's personal information. The best interests test should recognise that generating inferences for the purpose of informing professional educational support is a fundamentally different use from generating inferences for the purpose of advertising, profiling for commercial purposes, or sharing with third parties. The Code should not inadvertently create uncertainty about whether legitimate educational inference is consistent with best interests- it plainly is, provided the inferences are used to support the child and are subject to human review.

Part 3, Division 2 - Consent

Section 13: Consent given by child or person with parental responsibility

The age-of-consent threshold at 15 is appropriate and consistent with the OAIC's existing guidance. For school-based educational tools, the practical consent pathway is: the school establishes the

relationship, the parent or guardian provides consent for their child's participation, and the child is given age-appropriate information about what the service does. We want to raise a practical consideration about **Section 13(2)(b)**, which requires entities to "take reasonable steps to confirm that the person who gives consent is a person with parental responsibility for the child." In a school context, the most practical and privacy-preserving approach is for the school to manage the parent-child relationship as part of the enrolment process, rather than requiring the EdTech provider to independently verify parental identity. The school already has this information and has its own obligations to verify it. Requiring the technology provider to duplicate this verification would mean collecting additional sensitive information about parents (identity documents, proof of relationship) that the provider does not need and should not hold.
We would welcome guidance confirming that an EdTech provider may reasonably rely on a school's verification of parental responsibility where the service is accessed through a school-managed environment.

Section 14: Consent must be voluntary

We support the requirement that consent be voluntary, and we want to raise a practical tension that arises in educational contexts. When a school adopts an EdTech platform as its standard assessment or wellbeing tool, a parent's consent to their child's participation is technically voluntary - they can refuse. But the practical consequence of refusal may be that their child receives different, and potentially lesser, assessment support than their peers. The child doesn't choose whether their school uses the tool. The parent's "choice" exists within a context where the alternative is opting their child out of a service the school has determined is beneficial.

The Explanatory Statement notes that consent is not voluntary where "the individual will be unable to access the entity's service" if they refuse. In a school context, the child doesn't lose access to education, but they may lose access to the specific assessment and support that the tool provides. This is a meaningful consequence, and it creates a grey area around voluntariness.
We suggest the Code or its guidance acknowledge this tension directly. One approach would be to recognise that in school-managed contexts, the school's duty of care and educational obligations can provide a lawful basis for processing under the Australian Privacy Principles, with parental consent operating as an additional safeguard rather than the sole legal ground. This would mean that a parent who withholds consent prevents the tool from processing their child's data, but the school retains responsibility for providing equivalent support through other means. The consent is genuinely voluntary because refusal doesn't leave the child unsupported - it just means the support comes through a different channel.

This distinction matters for neurodivergent children in particular. A parent of an autistic child may have legitimate concerns about how their child's data is handled by an EdTech platform. That concern should not force them into a choice between data privacy and educational support. The Code should ensure that both can coexist.

Section 15: Consent must be informed- and Section 15(4): 12-month maximum

We strongly support the 12-month maximum consent period. For school-based services, this aligns naturally with the school year cycle. Annual consent renewal gives parents and children a regular opportunity to reconsider their participation, ensures consent remains current, and prevents the accumulation of stale or forgotten permissions.

Section 17: Consent can be withdrawn

We support the right to withdraw consent at any time and the requirement for a clear, simple, and accessible withdrawal mechanism. For educational tools, we want to flag a practical question about what withdrawal means for data that has already been collected and processed.
When a parent withdraws consent for their child's participation in an observation-based platform like ours, the straightforward elements are clear: the entity must stop collecting new observations, stop generating new inferences, and stop providing the service in relation to that child. **Section 17** handles this well.

The less straightforward question is what happens to data that was collected and processed while consent was active. An observation recorded three months ago has already been used to inform the system's understanding of the child. Inferences have been generated. Those inferences may have informed follow-up questions that the teacher has already asked, and support strategies that have already been implemented.

We suggest the Code or its guidance clarify that withdrawal of consent should trigger:
-Immediate cessation of new data collection and processing for that child.
-An offer to the parent to choose between anonymisation and deletion of existing data, consistent with the destruction right in **Section 32**.
-Where the parent chooses deletion, cascading destruction of both the raw observations and any inferences derived from them.
-Where the parent chooses anonymisation, de-identification of the child's records so they cannot be re-associated with the child, but aggregate patterns can be retained for service improvement where this is consistent with the entity's other obligations.

The key principle is that withdrawal should be meaningful and comprehensive, not merely prospective. A parent who withdraws consent should not have to separately invoke the destruction right in **Section 32** to deal with historical data - withdrawal should itself trigger a clear process for addressing what already exists.

Section 18: Consent must be specific

We support the requirement that consent be specific and for a distinct purpose. For educational technology, this provision has particular practical significance.

In an observation-based platform like ours, there are several distinct purposes for which children's data may be processed, and a parent should be able to consent to each independently:
-Consent to observation recording: the teacher records what they observe about the child.
-Consent to automated inference: the system analyses observations and identifies relevant developmental dynamics, generates follow-up questions, and suggests support strategies.
-Consent to longitudinal profiling: the system builds an ongoing understanding of the child's development over time, across observations and across school terms.
-Consent to contribution to service improvement: anonymised data from the child's use contributes to improving the platform for other children.

These are genuinely different purposes, and a parent may reasonably consent to some but not others. A parent who is comfortable with their child's teacher recording observations may be less comfortable with automated inference. A parent who accepts both may draw the line at their child's data contributing to product improvement.

The Code's prohibition on bundled consent requests in **Section 14(3)(b)** supports this reading - seeking a single consent for all four purposes would not meet the specificity requirement. We

welcome this and would encourage the OAIC to provide guidance confirming that EdTech providers should offer granular consent options that allow parents to meaningfully distinguish between the core educational service and any additional processing.

We note that this creates a design obligation: the system must be architecturally capable of providing different levels of service depending on which consents have been granted. A parent who consents to observation recording but not automated inference should receive a service that records observations without generating algorithmic recommendations. This is achievable, but it needs to be designed in from the start - it cannot be retrofitted easily. The Code's "strictly necessary" standard in **Section 9** and the privacy-by-default obligation support this approach.

Section 20: Assent of child under 15 years

The assent requirement is thoughtful. It recognises that children under 15 should have a voice in decisions about their personal information even where legal consent rests with a parent. For educational tools, this means giving the child age-appropriate information about what the service does and an opportunity to express their view, which is exactly what we believe good practice looks like. We do want to note that the assent requirement needs to be applied with sensitivity to children's developmental differences. A child with an intellectual disability or significant developmental delay may not be able to engage with an assent process designed for their chronological age. The Code or its guidance should explicitly acknowledge that assent processes must be adapted to the child's developmental capacity, not just their age, and that the inability of a particular child to provide assent does not prevent the entity from providing the service where parental consent has been obtained and the service is in the child's best interests.

Part 3, Division 3 · Transparency

Section 23: APP privacy policy requirements

We support the requirement for a child-directed version of the privacy policy. The specific requirements - clear, concise, transparent, age appropriate, no complex or technical language, non-text material where appropriate - are all sensible. For services where the child is primarily a data subject rather than a direct user, we suggest the Code or its guidance clarify what form the child-directed privacy policy should take. A child whose teacher uses our engine to record observations about them may never directly interact with the platform's interface, but they still have a right to understand what information exists about them and how it is being used. In practice, this might mean the child-directed privacy information is delivered through the school or parent rather than through the service's interface - and the Code should recognise this as a valid approach.

Section 28: Right to request information about handling of personal information

This is one of the most important provisions in the Code for our context. **Section 28(2)(g)** specifically provides that a child or parent may request information about "whether there is any automated decision-making, including profiling, relating to the personal information and, if so, clear and meaningful information about the context of such decisions, including the logic involved and the consequences of making them." We welcome this provision. We are developing tools to use automated processing to identify which developmental dynamics are relevant to a teacher's observation, to generate follow-up questions, and to recommend evidence-based support strategies. None of these are "decisions" about the child in the consequential sense - they are suggestions for the teacher's professional consideration. But they are a form of automated processing that uses the child's personal information, and parents and children have every right to understand how that processing works.

We want to make a practical suggestion. The Explanatory Statement notes that an entity is "not expected to provide all details about the technologies used for automated decision-making or profiling" but that "information about the logic must be meaningful to an individual, without requiring them to have any technical knowledge." For educational tools, meaningful disclosure should include: what data goes in (observations from teachers and parents), what comes out (suggested developmental dynamics, follow-up questions, support recommendations), and the nature of the processing in between (in our case, semantic matching and adaptive assessment using item response theory). It should not require disclosure of proprietary algorithms or model weights, but it should give a parent enough understanding to form a view about whether the processing is appropriate for their child. We would welcome OAIC guidance on what constitutes "clear and meaningful information about the logic involved" for services that generate inferences about children through automated processing. This guidance would benefit not only our sector but any sector using AI or algorithmic processing in relation to children's data.

Part 3, Division 4 - Access to, and correction of, personal information about children

Section 30: Access requests

We support the 30-day response requirement. For school-based services, access requests are most likely to come from parents, and a 30-day turnaround is achievable.

Section 31: Correction requests

Correction in observation-based contexts requires particular care. When a teacher records an observation in our system- “Liam seemed distressed at drop-off this morning and threw his bag across the room" - this is the teacher's professional observation. It is a data point with its own integrity. If Liam's parent disagrees with the characterisation, the appropriate response is not to delete or alter the teacher's observation, but to allow the parent to add a note providing additional context or a different perspective. The corrected record should travel with the original observation so that anyone reviewing the data can see both viewpoints. We believe the Code's correction framework, which operates under APP 13.1 and 13.4, is flexible enough to accommodate this approach. But we would welcome explicit guidance confirming that correction of observation-based data about children can include the addition of contextual annotations rather than requiring modification or deletion of the original observation.

Part 3, Division 5 - Destruction of personal information about children

Section 32: Request to destroy

We support the destruction right. Children and parents should be able to request that personal information about a child be dealt with, and the entity must respond. However, for observation-based educational platforms, we would encourage the Code or its guidance to explicitly recognise de-identification as a legitimate alternative to full destruction, offered as a choice to the requesting parent.

Here is why this matters. In an observation-based system, individual observations contribute to patterns that benefit the child themselves and, when fully de-identified, may benefit other children. An observation like “a child became dysregulated after an unannounced change to the classroom layout" - stripped of all identifying information (name, school, age, date, any distinguishing details) - retains educational value as a general example of how environmental changes can affect children. The privacy risk is eliminated. The learning is preserved.

We suggest the Code or its guidance clarify that when a parent requests destruction, the entity should:
-Explain clearly what destruction means - the complete and irreversible removal of all personal information about the child, including observations, inferences, and any derived profiles.
-Offer de-identification as an alternative - the complete removal of all identifying information so the data can no longer be associated with the child, while retaining the anonymised observation for educational purposes.
-Respect whichever option the parent chooses. If the parent wants full destruction, the entity must comply. De-identification is an option, not a default.

We also want to flag the multi-subject consideration. When a teacher records an observation that mentions multiple children - "Emma and Sophie had an argument during group work" - a destruction request from Sophie's parent creates a question about what happens to the observation as it relates to Emma. We suggest that where destruction of one child's data can be achieved without affecting another child's data (for instance, by removing Sophie's name and identifying details), that is preferred. Where the observation is inseparable, the entity should notify the requesting parent and offer alternatives including anonymisation of their child's involvement.

This approach is consistent with the child's right to have their data removed while also acknowledging that observation-based educational data, properly de-identified, can serve the broader educational mission without any privacy cost to the individual child.

Part 3, Division 6 · Notification requirements for control or monitoring mechanisms

Section 33: Monitoring notification

We support the requirement to notify children when their service use is being monitored or controlled. For educational tools used under teacher supervision, this means being transparent with children about the fact that their interactions are visible to their teacher and, where applicable, their parents. We note that this provision applies specifically to monitoring of "service use" and "geolocation data." For services like ours, where the primary data is observations recorded by adults about children rather than the child's own service usage, the monitoring notification obligation may be limited.

Part 3, Division 7 · Making inquiries and complaints

Section 36: Child-friendly inquiry and complaints processes

We support this requirement. The obligation to allow anonymous or pseudonymous complaints is sensible, as is the 30-day response timeframe. For educational contexts, we would add that the complaints process should also be accessible to parents and guardians on behalf of children who may not have the capacity or confidence to raise a concern themselves, and the Code's definition of "persons" in **Section 36(2)(b)** appropriately covers this.

Part 3, Division 8 · Privacy Impact Assessments and privacy education and training

Section 38: Privacy Impact Assessments

We strongly support the PIA requirement. For services handling children's sensitive information, PIAs should be conducted before launch and before any significant change to data handling practices. We want to suggest an addition to the PIA framework. **Section 38(2)(f)** requires an assessment of "the risk of harm to, and the potential impact on, children resulting from the handling

of their personal information," and the Note helpfully specifies that harms may include "those of a physical, emotional, developmental or material nature." We would urge the OAIC to include in its guidance that the risk of harm assessment should specifically consider:
-The risk of inappropriate labelling or categorisation (for example, a system that generates inferences about a child's developmental profile creates a risk that those inferences are treated as diagnoses or permanent characteristics rather than as contextual, time-bound observations).
-The risk of deficit framing (presenting a child's profile in terms of what they cannot do rather than what supports they would benefit from).
-The risk of bias in automated processing (whether the system's inferences perform equitably across different cultural, linguistic, and neurodevelopmental backgrounds).

These are not speculative risks. They are the primary harms that educational data systems pose to children, and they deserve explicit attention in the PIA framework.

Section 39: Register of privacy impact assessments

The requirement to publish the PIA register online is a strong transparency measure and we support it.

Section 40: Privacy education and training

We support the annual training requirement. For educational tools, this obligation should extend not just to the entity's own staff but to guidance for the schools and educators who use the platform. If a teacher is recording observations about children using our tool, they are handling children's personal information within the meaning of the Act, and they should understand their obligations in doing so.

PROVISIONS NOT ADDRESSED IN THE EXPOSURE DRAFT

There are two matters we believe the Code should address that are not currently covered:

1. Cross-border data flows for children's sensitive information. **Section 26** addresses how entities must inform children about cross-border disclosures, but does not impose additional substantive requirements on those disclosures beyond what APP 8 already requires. Given the sensitivity of children's personal information - particularly health, wellbeing, and developmental data - we believe the Code should establish a stronger position. At minimum, entities should be required to document and justify any cross-border transfer of children's sensitive information, and to prefer Australian sovereign data hosting where available.

2. Secondary use of children's data for model training or product improvement. The "strictly necessary" standard in **Section 9** goes some way toward addressing this, but we believe the Code would benefit from an explicit statement that children's personal information collected for educational support purposes may not, by default, be used as training data for machine learning models, aggregated for product improvement, or contributed to data sets beyond what is needed for that child's service. This is a live concern in EdTech, where some platforms use classroom data to improve algorithms that are then sold to other customers.

CLOSING

We support the Code and want it to succeed. It will establish Australia as a leader in children's online privacy protection, and it will create a framework that responsible technology providers can build to rather than work around.

Ablative is at an early and deliberate stage of development. We are designing our privacy architecture now, with this Code in mind. We would welcome the opportunity to engage further with the OAIC, including:

-Demonstrating our platform's privacy-by-design approach as a practical reference example for how EdTech services can comply with the Code.
-Participating in any working groups or reference panels as the Code moves toward registration.
-Contributing to guidance material development, particularly in relation to educational technology, observation-based data, and automated processing of children's information.

We commend the OAIC's commitment to centring children in these protections, and we look forward to the Code's registration in December 2026.

[redacted]
Co-Founder, Ablative Pty Ltd

ABOUT ABLATIVE

Ablative is an Australian technology company. One of our current developments is an engine, which- amongst other things- will be applied to a usage around educational assessment and wellbeing. This will be a platform for use in schools and early childhood settings, with a particular interest in neurodiverse children. This engine is being designed to support the learning, development and wellbeing of children through continuous, observation-based profiling conducted by teachers and parents. Members of our team have a genuine vested interest, through lived experience, in this area and the areas that the Code deals with.

We are not a social media company, an advertising platform, or a general consumer app. We are building a tool that sits squarely within the category described in Note 1 to **Section 5** of the Exposure Draft: an application that tracks early childhood development and monitors student performance. The questions raised by this Code are not theoretical for us · they directly shape the architecture and design decisions we are making right now.

We have a particular focus on neurodivergent learners. Our platform is built around positive language framing, evidence-based recommendations, and a human-in-the-loop design philosophy where the system informs professional judgement rather than replacing it.

We acknowledge the OAIC's careful, consultative approach to developing this Code. Children's privacy is not an area that benefits from vague principles or good intentions- it requires specific, enforceable obligations, and we are pleased to see this Exposure Draft deliver them.