# Submission on the Exposure Draft of the Children's Online Privacy Code – Independent Schools Australia and National Catholic Education Commission

*5 June 2026*
*Submit via email: copc@oaic.gov.au*

## Introduction

This submission on the Exposure Draft of the Children's Online Privacy Code (the **Code**) is made on behalf of Independent Schools Australia (ISA) and the National Catholic Education Commission (NCEC) (together, **we**, **our**), the peak national bodies representing Australia's independent and Catholic school sectors respectively. These sectors comprise approximately 2,900 non-government schools (**Schools**) located across all Australian states and territories. We welcome the opportunity to contribute to the development of the Code and support its objective of strengthening privacy protections for children.

ISA and NCEC are deeply committed to protecting the privacy of children and take a proactive approach to providing guidance to our Schools on privacy compliance, including in relation to children's personal information handled in the online environment. In particular, since 2001 we have published and regularly updated a joint national privacy compliance manual (Privacy-Compliance-Manual-2023.pdf) (**PCM**), which provides detailed, bespoke guidance and practical examples tailored to the unique circumstances in which Schools operate.

It is also relevant that Education Services Australia (**ESA**) has standardised the assessment of digital products and services to determine their suitability for use in schools (both government and non-government).

Schools operate in a unique and complex environment, which has no parallel in consumer-facing commercial organisations. Schools must balance privacy protections with their duty of care to students, mandatory reporting obligations, child safety requirements, and educational and welfare responsibilities.

There are a number of unintended consequences of the Code as it relates to Schools, including the following:

1. it may be contended that the Code applies to Schools themselves, not just to their online service providers, in light of uncertainty regarding who is the 'provider' of certain online services;

2. online service providers are likely to contractually pass down to Schools certain obligations under the Code that the providers are unable to discharge themselves;

3. if the Code does apply to Schools directly and/or the Code's obligations are contractually passed down to Schools, there are a number of consequences for Schools, teachers, parents and students which we believe are unintended. In this respect, whilst the Code expressly references '*online school management systems*' as an example of a service regulated by the Code, its specific obligations and illustrative examples within the Exposure Draft of the Explanatory Statement (**Explanatory Statement**) appear principally designed for consumer-facing commercial online services. This leads to the concern that the Code may have disproportionate and unintended consequences in the school environment, where online services are typically selected, configured and governed by Schools rather than children, and are integral to fulfilling Schools' core educational, welfare and safeguarding functions and obligations.

4. in a number of instances, strict application of the Code within Schools may not serve the best interests of a child, or may impede Schools' ability to act in the best interests of other children in their care. This is explained further under the heading '*Implications of the Code in the School environment*' below; and

5. in light of the comprehensive guidance already contained in the PCM, there is a risk that requiring Schools to implement the obligations in the Code may yield limited additional protection of

children's privacy, whilst potentially producing outcomes that may not be in the best interests of a child, delaying action that is in the best interests of a child, increasing confusion for Schools, staff, students and parents, and imposing disproportionate administrative burden.

The complex nature of Schools necessitates a principles-based approach, rather than prescriptive rules and rigid thresholds. We submit that the Code is, in its current form, unworkable in the school environment.

Considering:

1. the significant, detailed and bespoke guidance already contained in the PCM;

2. the software assessment process of the ESA;

3. the disproportionate and unintended consequences of the Code for Schools and their community (including children within their community); and

4. the risk that, even if Schools are specified as a class of APP entities that are not bound by the Code, technology providers may nevertheless contractually require Schools to perform compliance functions on their behalf, thereby extending the application of the Code to Schools through indirect means,

we:

(a) submit that pursuant to subsection 26GC(7) of the *Privacy Act 1988* (Cth) (**Privacy Act**), Schools be specified in the Code as a class of APP entities that are not bound by the Code; and

(b) request that, in light of the contractual pass-down risk, the OAIC consider what amendments can be made to the Code to ensure it achieves its objective of strengthening privacy protections for children, whilst remaining workable in the school environment and not producing unintended or disproportionate consequences. By way of example, this might be achieved by limiting section 5 to services likely to be accessed by a Parent (noting that services likely to be accessed by children would already be regulated by the Code under section 26GC(5) of the Privacy Act). If the Code only applied to services likely to be accessed by children or a Parent, this would go some way to reducing the number of obligations that the providers would be unable to discharge themselves and would therefore seek to pass on to Schools. However, we acknowledge that this policy concern warrants careful consideration of what amendments to the Code may be appropriate to address it. We would value the opportunity to work constructively with the OAIC on this matter.

If the OAIC does not consider it appropriate to specify Schools as a class of APP entities that are not bound by the Code, we request guidance on the meaning of 'provider' and a further opportunity to provide detailed submissions on each of the provisions of the Code and how it would affect Schools.

## Outline of submission

This submission is set out in four parts:

1. Part A contains a brief overview of IT platforms used by Schools in their day-to-day operations for context to this submission;

2. Part B contains a further explanation of the PCM and our approach to updating it, including in light of the Code, as well as a further information regarding ESA's software assessment process;

3. Part C contains examples of the implications of the Code in the school environment;

4. Part D contains submissions or comments regarding the application of the Code, in particular regarding:

    (a) the planned exemption for Schools that provide a health service;

    (b) the meaning of 'provider'; and

    (c) developing a workable outcome for Schools in light of the contractual pass-down risk.

## Part A: IT platforms used by schools

This submission should be viewed in the context of the large number of IT platforms currently used by Schools in their day-to-day operations. Some are accessed by children and/or their Parents. Some are not and are only accessible by teachers and school staff. Many of these platforms may arguably be regulated by the Code, depending on its final drafting and interpretation. The Code itself provides the example of online school management systems that monitor student performance. Other examples include (to the extent they are delivered online):

1. learning management systems, and other online teaching, learning and creative platforms;
2. school administration and student records systems;
3. student and parent communication and collaboration tools;
4. lunch order applications;
5. assessment and learning analytics tools;
6. virtual classrooms;
7. safety, wellbeing and pastoral care systems; and
8. the School website and social media platforms.

Whilst some of the above tools may not currently be 'online' in the sense regulated by the Code, the distinction between online and offline services is increasingly blurred.

## Part B: The PCM and ST4S

The PCM assists and guides Schools with privacy compliance by providing detailed commentary on the steps Schools should take to comply with their privacy obligations, in particular those arising under the Privacy Act. It includes practical, bespoke guidance specific to situations Schools face, as well as template compliance documents. It is publicly available to support transparency with our school communities. The PCM was first published in 2001 and is updated as laws and information handling practices evolve. Every School has access to the PCM via the ISA and NCEC websites.

The PCM has been updated to reflect the OAIC's Australian Privacy Principles (**APPs**) Guidelines and other guidance issued by the OAIC. In addition, once the Code is finalised — regardless of whether Schools are specified as a class of APP entities that are not bound by the Code — ISA and NCEC commit to reviewing the PCM with a view to considering whether it is appropriate to incorporate any requirements of the Code as guidance on steps that Schools should consider taking as best practice. This commitment reflects our genuine desire to advance appropriate children's privacy protections in the school environment through practical, effective guidance.

As a recent example of the practical guidance that Schools derive from the PCM, we note that certain Schools that utilise the Canvas platform contacted us for guidance following the recent Canvas cyber incident. We were able to promptly refer those Schools to the PCM's comprehensive guidance on data breach response and compliance with Part IIIC of the Privacy Act.

In addition, ESA on behalf of state and territory governments and the Catholic and Independent school sectors and the New Zealand Ministry of Education have developed ST4S (Safer Technologies 4 Schools) to enhance security, privacy, interoperability and online safety of software products and services commonly used by Australian and New Zealand schools. ST4S has a working group made up of security and privacy professionals across Australia and New Zealand. We believe 770 software vendors have submitted software for evaluations. ST4S assessments already include comprehensive assessments of privacy, security and governance. If you would like more information about ST4S, we would be happy to provide this. It should be noted that ST4S has been developed for the benefit of all schools, both government and non-government; in contrast to the application of the Code.

Additionally, the Australian Education Research Organisation (AERO) has partnered with ESA to support the alignment of edtech tools with the evidence on effective teaching practices through progressing work on a national quality assurance education standards. The quality assurance education standards have been developed with a primary focus on supporting effective student learning in Australian classrooms. It will complement ESA's Safer Technologies 4 Schools (ST4S) and other initiatives to assure schools and systems about which products are safe, responsible and educationally effective.

## Part C: Implications of the Code in the school environment

The principles-based nature of the Privacy Act is well suited to the school environment. It provides the flexibility necessary for Schools to protect children's privacy whilst appropriately balancing their privacy obligations with their duty of care to students, mandatory reporting obligations, child safety requirements, and educational and welfare responsibilities.

A number of provisions of the Code impose prescriptive requirements that may be difficult to reconcile with the nuanced school environment and may, in certain circumstances, produce outcomes inconsistent with the privacy and welfare objectives the Code seeks to achieve. Set out below are illustrative examples of what we submit are disproportionate and unintended consequences of the Code in the school environment. These examples should not be taken as endorsement of the remaining provisions. If the OAIC does not consider it appropriate to specify Schools as a class of APP entities that are not bound by the Code, we request a further opportunity to provide detailed submissions on the impact of each provision (including further submissions on the provisions discussed below).

### *1. Strictly necessary consideration for default settings (section 9)*

Section 9(1) provides that an entity must implement technical and organisational measures that ensure that, by default, the entity only collects, uses or discloses personal information about a child that is strictly necessary to provide the entity's service. The Explanatory Statement indicates that '*strictly necessary*' means '*essential to provide the service*'.

We acknowledge that the Explanatory Statement provides that section 9 does not narrow or restrict the operation of APP 3.1 or 3.2, and that section 9 is directed only to the **default** design of services.

However, even on this understanding, section 9(1) presents significant practical difficulties for Schools, including:

1. it may be difficult for a School to differentiate between default and non-default collection, use and disclosure;

2. even where a **service** can technically be provided without handling certain information, **a School may be unable to perform its functions or discharge its obligations** without handling that information;

3. it may be impossible for a school to modify the software platform to prevent collection of the information;

4. given that students and parents frequently provide information without solicitation, the absence of any exception in section 9 for unsolicited information may create practical difficulties — for example, in relation to the design of services that include free-text fields through which unsolicited personal information may be entered.

For example, a School may use an online learning management system to deliver educational content to students. It may be contended that the service can technically be 'provided' without collecting or using information about a student's learning progress, engagement patterns or accessibility needs. However, a School may be unable to discharge its duty of care, identify students at risk of disengagement, or provide appropriate adjustments for students with additional learning needs without that information being collected and used by default. Similarly, free-text fields are an inherent and necessary feature of communication and assessment platforms used by Schools. By their nature, such fields cannot be constrained to elicit only information that is 'strictly necessary' for the provision of the service. A student may, for instance, disclose information about family circumstances, behavioural issues involving other students, or reasons for absence — information which it might be contended is not strictly necessary to provide the service, but which is reasonably necessary for the School's functions or activities and which the School may be obliged to act upon once received.

Section 9(2) provides that the measures in section 9(1) must enable an end-user of the entity's service who is a child to control whether personal information about the child is collected, used or disclosed where that information is not strictly necessary for the provision of the entity's service.

The Explanatory Statement describes this as enabling children to '*turn on or off additional elements such as personalised content, targeted advertising or recommendations that rely on the handling of a child's personal information*'. However, section 9(2) arguably has a broader application than the Explanatory Statement suggests.

Whilst the choice afforded by section 9(2) may be appropriate for optional, consumer-facing features, it is fundamentally incompatible with the school environment, where online services facilitate core functions such as enrolment, attendance monitoring, student wellbeing, communication with families, academic assessment, learning analytics and personalised educational support. For each of these services, Schools would need to undertake the significant task of determining whether each type of personal information collected, used or disclosed by default is strictly necessary for the provision of the service. This difficulty is compounded by the fact that, even where a service can technically be provided without handling certain information, a School may be unable to perform its functions or discharge its obligations without that information being handled by default.

## *2. Best interests (section 10)*

Section 10 requires, in summary, that the collection of personal information about a child be consistent with the best interests of that child.

Whilst we strongly support the principle of acting in children's best interests — a principle with which our Schools have extensive practical experience — this provision may not accommodate the nuanced circumstances in which Schools collect personal information.

Schools must support the wellbeing and education of hundreds to thousands of students simultaneously. A singular focus on whether collection is in the best interests of one child may come at the expense of the health, safety or wellbeing of other children in the School's care. Schools are frequently required to make decisions involving the handling of personal information for legitimate and protective reasons — for example, monitoring online behaviour to prevent cyberbullying, or sharing information with staff to prevent harm to other students.

Whilst section 10(6) provides exceptions where, relevantly, collection is required or authorised by law or court/tribunal order, where a permitted general situation exists, or where a permitted health situation exists, these exceptions may not address every situation a School encounters. This may create uncertainty for Schools that must routinely balance the interests of one child against the interests of others, and may lead to a risk that Schools limit legitimate collection or delay action out of concern that their decisions could later be contested — an outcome that would be counterproductive and may undermine the very child-centred outcomes the Code seeks to promote.

Furthermore, what constitutes 'the best interests of the child' may be open to differing interpretations in the school context. Actions undertaken by a School in good faith and for a legitimate purpose may be challenged by Parents or students who hold a different view of what is in their or their child's best interests. It is also not uncommon for two parents to have different views about the best interests of a child. Requiring Schools to engage in ongoing assessment of, or dialogue with Parents about, what is or is not in a particular child's best interests may be impractical and may divert resources from core educational and welfare functions.

## *3. Removal of exception for uses and disclosures (section 11)*

Section 11 provides that, in complying with APP 6.1, an entity must not use or disclose personal information about a child unless the child has consented and the use or disclosure is consistent with the best interests of the child.

We repeat our comments regarding the best interests of the child in respect of section 10 above.

In addition, we are concerned that, based on the drafting of section 11 and the guidance in the Explanatory Statement, entities regulated by the Code will no longer be permitted to use or disclose personal information in accordance with APP 6.2(a) — that is, for a related (or directly related, in respect of sensitive information) secondary purpose that the child would reasonably expect. In the school context, there are many secondary uses and disclosures of personal information that do not interfere with a child's privacy and are necessary to ensure the School can function effectively. For example, administration, providing reports to parents, seeking technical support, assessing eligibility for and applying for funding and government grants, and assessing and managing learning difficulties may, in some cases, constitute secondary purposes.

We also submit that the Explanatory Statement should confirm that section 11 is not intended to require consent where personal information of a child is used or disclosed for the primary purpose for which it was collected.

## *4. Consent (section 13)*

Section 13(1) provides that consent to the collection, use or disclosure of personal information about a child may be given by the child only if the child is at least 15 years of age. If the child is under 15 years of age, the entity must obtain consent from a Parent.

Schools must constantly manage complex family situations, including shared parental responsibility arrangements, family violence situations, and circumstances where a child is sufficiently mature to provide their own consent. Prescriptive rules about consent may present significant challenges in such circumstances.

There are also circumstances where requiring consent from a Parent would cause harm to a student under 15 who has the capacity to consent — for example, where a student discloses family violence or abuse. The exceptions in section 13(4) are limited to circumstances where the child is seeking legal or health-related information or support in connection with a Parent, or if a law permitted a child under 15 years of age to consent. These exceptions are narrow and do not provide the flexibility needed for the varied and sensitive circumstances Schools encounter.

We consider the OAIC's current guidance on determining whether a child has capacity to consent, which is reflected in the PCM, to be appropriate and sufficiently adaptable to the unique circumstances and family situations that Schools regularly navigate.

## *5. Notice to children (section 13(3))*

Section 13(3) requires that if a Parent consents to the collection, use or disclosure of personal information about a child, the entity must provide an age-appropriate notice to the child stating certain information. The Explanatory Statement states that this requirement responds to feedback received from children during OAIC consultations indicating that children want greater transparency over how their personal information is handled and wish to be more involved in the consent process to improve their digital literacy and privacy education.

While this objective is commendable in a consumer-facing context, Schools collect, use and disclose student information on an ongoing basis, and requiring an age-appropriate notice to the child each time parental consent is relied upon may be administratively impractical and lead to notification fatigue.

Providing privacy notices directly to children — particularly younger students — may create confusion, give the impression that the child can override parental consent, or affect the relationship of trust between the student, their parents and the School. A very young child is unlikely to comprehend such a notice (no matter how 'age-appropriate' it is drafted) and may simply pass it to their parents, who must then reconcile the information provided during the consent process with the differently worded age-appropriate notice given to the child.

The current approach under the Privacy Act allows Schools to provide parents with clear, consolidated information. The section 13(3) approach may create significant administrative burden, as parents may be confused by differences between the information provided to them and the age-appropriate information provided to their children, potentially leading to unnecessary enquiries and complaints.

## *6. Collection, use and disclosure — assent requirement (section 20)*

Section 20 introduces a requirement, not contemplated by the APPs, to seek the assent of certain children in certain circumstances.

Critically, whilst we acknowledge that the Explanatory Statement states that a child's assent is not required where a Parent has already provided consent for a specific purpose, section 20 does not incorporate the appropriate and balanced exceptions contained in APPs 3.4 and 6.2. Those exceptions recognise that there are legitimate circumstances in which personal information may be collected, used or disclosed without consent. In the school environment, requiring assent for every secondary use or disclosure that falls within section 20 — without the benefit of these exceptions — may impede Schools' ability to act promptly in the interests of children, particularly where information must be handled for purposes that a child would reasonably expect.

In addition, the practical operation of assent requirements for younger children may present particular challenges in school contexts where parental consent has already been provided through enrolment and ongoing education delivery processes.

## Part D: Application of the Code

### *Health service providers*

Many Schools provide a health service and may therefore not be bound by the Code by operation of subsection 5(c) of the Code and subparagraph 26GC(5)(a)(iii) of the Privacy Act. The view that certain Schools are health service providers is supported by OAIC guidance (What is a health service provider? | OAIC).

However, to avoid uncertainty — particularly regarding how these provisions interact with section 7 of the Code (which applies the Code to specific activities of an entity rather than the entity as a whole) — we repeat our submission that Schools should be specified in the Code as a class of APP entities that are not bound by the Code, rather than relying on the health service provider exclusion alone.

### *Uncertainty regarding the meaning of 'provider' in the school context*

There is uncertainty regarding who constitutes the 'provider' of a service in the school context. Whilst it is understood that 'provider' should be interpreted consistently with its meaning under the *Online Safety Act 2021* (Cth), there appears to be limited guidance on the meaning of that term under that Act, at least in a manner that would assist in determining its application to Schools. This uncertainty is heightened in the school environment, where Schools require or facilitate the use of online tools, often determine which students will use a service, and control what types of personal information flow into and out of an online platform.

The question arises whether a School 'provides' a service by making it available to its students, determining which students are permitted to use it, and controlling what types of personal information flow into and out of the service — notwithstanding that the School has no involvement in the development, operation or maintenance of the technical architecture of the tool, and therefore no ability to implement certain obligations in the Code (in particular, the technical measures required under section 9).

This difficulty is compounded by the fact that, in the school context, it is difficult to determine who the 'provider' is based on the operation of the obligations in the Code. We submit that some obligations could only be implemented by the School's third-party vendors (for example, implementing technical default settings under section 9), whilst other obligations could realistically only be implemented by the School, if this were possible (as explained under the heading '*Section 5*' above). This division of obligations between Schools and their vendors may be difficult to reconcile with a single entity being the 'provider' for the purposes of the Code.

If the OAIC does not consider it appropriate to specify Schools as a class of APP entities that are not bound by the Code, we request guidance on the meaning of 'provider'.

### *Policy consideration: mitigating unintended extension of the Code to Schools through contractual mechanisms*

In light of the risk that online service providers might contractually pass down to Schools certain obligations under the Code that the providers are unable to discharge themselves, we request that the OAIC consider what amendments can be made to the Code to ensure it achieves its objective of strengthening privacy protections for children, whilst remaining workable in the school environment and not producing unintended or disproportionate consequences. The basis for this request is set out below.

In the Report of the Attorney-General's Department's *Privacy Act Review*, a range of recommendations were made aimed at strengthening children's privacy protections online under the Privacy Act. This included the recommendation to mandate the development of a Children's Online Privacy Code, applying to online services likely to be accessed by children. This intention is achieved through section 26GC(5) of the Privacy Act, which means that the Code applies to online services likely to be accessed by children, including the types of services that would be caught by section 5 of the Code to the extent that they are likely to be accessed by children. However, the practical effect of section 5 of the Code is that the Code is extended to online services that are **not** likely to be accessed by children. It is unclear how this achieves the policy objective. Such services are already regulated by the Privacy Act and would, if section 5 remains in its current form, be subject to additional obligations under the Code.

In addition, many of the obligations in the Code may be difficult to implement by technology providers that fall within section 5 of the Code (but do not fall within subsection 26GC(5) of the Privacy Act), where those providers supply services to Schools and have no direct relationship with the child or Parent. Such providers may have limited visibility of the context in which the service is used and, in respect of many services used in Schools, limited means of communicating directly with the child or a Parent. As a result, they may face significant difficulty in determining whether information is 'strictly necessary', assessing whether collection is in the 'best interests of the child', implementing controls that enable a child to 'turn on or turn off' additional elements of the service, providing age-appropriate notices to children, or obtaining a child's assent.

Accordingly, even if Schools are specified as a class of APP entities that are not bound by the Code pursuant to subsection 26GC(7) of the Privacy Act, in practice such technology providers are likely to contractually require Schools to take many of the steps necessary to comply with the Code on the provider's behalf. This would effectively extend the application of the Code to Schools through contractual mechanisms, undermining the very purpose of specifying Schools as a class of APP entities that are not bound by the Code.

We note that this issue may also impact government schools where their technology providers attempt to contractually pass-down certain obligations under the Code to the schools.

Whilst we acknowledge this important policy concern requires careful consideration beyond this submission process, we provide below brief context regarding our example of amending section 5 to limit its application to services likely to be accessed by a Parent (noting that services likely to be accessed by children would already be regulated by the Code given its current scope under section 26GC(5) of the Privacy Act). This would:

1. ensure that the Code only captures services that are likely to be accessed by children or Parents, thereby excluding back-end services used by Schools. We consider that the most disproportionate consequences would be felt in respect of such back-end services; and

2. ensure that regulated service providers have a direct relationship with either the child or a Parent, and are therefore better placed to discharge their obligations under the Code.

## Conclusion

Considering:

1. the significant, detailed and bespoke guidance already contained in the PCM, and our commitment to reviewing the PCM to consider whether it is appropriate to incorporate any requirements of the Code as guidance on steps that Schools should consider taking as best practice;

2. the software assessment process of the ESA;

3. the disproportionate and unintended consequences of the Code for Schools and their communities (including children within those communities), including that strict application of the Code within Schools may not serve the best interests of a child, may impede Schools' ability to act promptly in the interests of children, and may produce outcomes inconsistent with the privacy and welfare objectives the Code seeks to achieve;

4. the risk that, even if Schools are specified as a class of APP entities that are not bound by the Code, technology providers may contractually require Schools to perform compliance functions on their behalf, thereby extending the application of the Code to Schools through indirect means,

we:

5. submit that, pursuant to subsection 26GC(7) of the Privacy Act, Schools be specified in the Code as a class of APP entities that are not bound by the Code; and

6. request that, in light of the contractual pass-down risk, the OAIC consider what amendments can be made to the Code to ensure it achieves its objective of strengthening privacy protections for children, whilst remaining workable in the school environment and not producing unintended or disproportionate consequences that may, amongst other things, undermine a School's ability to act in the best interests of a child. By way of example, this might be achieved by limiting section 5 to services likely to be accessed by a Parent (noting that services likely to be accessed by children would already be regulated by the Code given its current scope under section 26GC(5) of the Privacy Act). However, we acknowledge that this policy concern warrants careful consideration of what amendments to the Code may be appropriate to address it. We would value the opportunity to work constructively with the OAIC on this matter.

We wish to express our willingness to participate in any stakeholder consultation process, provide worked examples, or otherwise assist the OAIC in considering our submissions.

If the OAIC does not consider it appropriate to specify Schools as a class of APP entities that are not bound by the Code, we request guidance on the meaning of 'provider' and a further opportunity to provide detailed submissions on each of the provisions of the Code.

We reiterate our genuine commitment to advancing children's privacy protections in the school environment and welcome the opportunity to engage constructively with the OAIC in the further development of the Code.

[redacted]

**Chief Executive Officer**
Independent Schools Australia

**Executive Director**
National Catholic Education Commission