Education Development Centre
4 Milner Street, Hindmarsh SA 5007
[redacted]
Email: [redacted]
SAPPA ABN: 29 671 201 072

SAPPA Feedback on the Exposure Draft Children's Online Privacy Code 2026

Via: [redacted]

Dear [redacted]

Thank you for inviting the South Australian Primary Principals Association to provide feedback on the Exposure Draft Privacy (Children's Online Privacy) Code 2026.

SAPPA supports the intent of the proposed Code and the objective of strengthening protections for children's personal information. The principles of privacy by default, data minimisation, transparency, age-appropriate communication, meaningful consent and consideration of the best interests of the child are appropriate and timely.

Our feedback is focused primarily on the practical implications for schools and school leaders, including possible unintended consequences arising from the proposed consent, compliance and implementation arrangements.

While South Australian public schools may not themselves be directly bound by the Commonwealth Privacy Act in the same way as commercial service providers, the proposed Code is likely to have significant indirect effects through the software, platforms and online services used by schools.

The exposure draft expressly contemplates online school management systems and services concerned with children's activities. It is therefore important that the final Code and supporting guidance reflect the realities of school digital environments and avoid transferring provider compliance responsibilities to individual schools and principals.

The school digital environment

The digital environment within schools is not limited to a small number of centrally managed systems.

While the Department for Education procures a number of core platforms, licences and digital services, the centrally available offering is relatively basic. It is routine and often necessary for individual schools to procure additional online services that respond to local context and the needs of students, staff and families.

These can include platforms supporting:

- literacy and numeracy learning and intervention
- assessment, reporting and student progress monitoring
- learning management and digital portfolios
- communication with families
- student wellbeing and engagement
- inclusion and personalised learning

- curriculum-specific applications
- school administration and timetabling
- online safety and device management
- artificial intelligence-enabled learning and productivity tools

Schools may use multiple services, each with different terms, privacy settings, data arrangements and consent requirements. The cumulative impact of the proposed Code therefore needs to be considered, rather than the implications of each service being assessed in isolation.

Duration and administration of consent

SAPPA is particularly concerned by the proposal that consent may remain current for no more than 12 months.

For a school using multiple locally procured services, this could create an annual, platform-by-platform cycle involving:

- identifying which services require consent
- determining whether the purpose is strictly necessary or optional
- providing separate privacy notices
- obtaining and recording parental consent
- verifying that the person providing consent has parental responsibility
- seeking student assent where required
- following up non-responding families
- managing withdrawn consent
- restricting or restoring student access
- repeating the process each year

This would create a substantial recurring administrative burden for schools.

There is also a real risk that providers will seek to rely on schools to administer these processes because schools have established relationships with families. This would effectively transfer provider compliance obligations to principals, teachers and administrative staff.

Individual schools should not be required to interpret complex privacy requirements or act as compliance agents for commercial providers.

The proposed 12-month limit could also result in students losing access to valuable learning or support tools because a parent or carer has not completed an annual consent process, rather than because they have made an informed decision to refuse consent.

Schools already experience difficulty obtaining timely responses to routine forms and permissions. A lack of response does not necessarily indicate opposition. It may reflect limited digital access, language or literacy barriers, housing or family instability, competing pressures, shared or disputed parental responsibility, complex care arrangements or disengagement from school communications.

Students experiencing disadvantage may therefore be most likely to lose access to services intended to support their learning and wellbeing. A privacy protection framework should not unintentionally create a new barrier to educational participation.

The proposal may also discourage schools from adopting fit-for-purpose services. Schools may conclude that the administrative and legal risks associated with locally procured products are too great and retreat to a limited centrally available suite, even where those services do not adequately meet student or school needs.

This could reduce local responsiveness and innovation, limit access to specialist learning supports, widen inequity between schools and particularly disadvantage smaller, country and highly complex schools.

SAPPA recommends that consent remain valid while the purpose, information collected, disclosure arrangements and risk profile remain materially unchanged.

Fresh consent should be required where there is a significant change to:

- the purpose for which information is collected
- the types of personal or sensitive information collected
- the organisations to which information is disclosed
- overseas storage or processing arrangements
- the use of information for artificial intelligence or product development
- the level of monitoring, profiling or automated decision-making
- the risk to the child

Consent should not automatically expire after 12 months where nothing material has changed.

If the maximum 12-month period is retained, annual renewal should be centrally coordinated for approved education products through a common Department process. Individual schools and principals should not be expected to administer separate annual consent arrangements on behalf of multiple commercial providers.

Approved education services

SAPPA recommends that the OAIC, in consultation with education authorities, privacy regulators and the school sector, establish a framework for recognising approved education services.

Services included within this framework should be required to meet clear standards relating to privacy by design, data minimisation, cybersecurity, retention, deletion, overseas disclosure, artificial intelligence, commercial use and transparency.

Where an approved service is being used for a core educational, safeguarding or school administration purpose, consent should not automatically expire after 12 months. Consent should remain current while:

- the purpose for which the service is used remains unchanged
- the types of personal information collected remain materially unchanged
- disclosure and storage arrangements remain materially unchanged
- the service continues to meet the approved privacy and security standards
- student information is not used for advertising, unrelated commercial purposes or the training of general commercial artificial intelligence models

Fresh consent should be required where there is a material change to the service, its data-handling practices or its risk profile.

The OAIC could establish the criteria and assurance requirements for this framework, with an appropriate education authority or nationally recognised body maintaining a register of approved services. This would provide schools, families and providers with greater certainty while avoiding repetitive annual consent processes for established and appropriately assessed educational services.

Responsibility and accountability

The final Code should provide greater clarity about the respective responsibilities of commercial providers, education departments, individual schools, principals, parents and students.

It may not always be clear who is considered the provider of a service where:

- the Department purchases a product for system-wide use
- a school purchases a licence locally
- a vendor integrates with a departmental platform
- staff use a free or low-cost online service
- a product is accessed through a school-managed device
- student information is transferred between systems

The final Code and supporting guidance should confirm that the ordinary procurement or use of a third-party service by a school does not make the school or principal the provider of that service.

Responsibility for compliance should remain primarily with the entity that designs, operates and controls the service and determines how personal information is collected, used, stored and disclosed.

Verification of parental responsibility

The proposal requiring providers to take reasonable steps to confirm that consent has been provided by a person with parental responsibility may be difficult to administer in school communities.

Complex circumstances may include shared or disputed parental responsibility, parenting and court orders, family violence, estranged parents, guardianship arrangements, children under the guardianship of the Minister, kinship care, informal care and changes in family circumstances.

The explanatory material suggests that verification could occur through a token supplied by a school. SAPPA would be concerned if schools were expected to certify or verify legal parental responsibility for the purposes of a commercial provider's compliance.

Schools should not assume this role unless there is clear legal authority, a secure and standardised process, Departmental oversight, specialist advice, protection from liability and no additional administrative burden at the local level.

Any verification arrangements should be managed centrally wherever possible.

Core educational purposes and optional uses

The final Code should more clearly distinguish between information handling necessary for core public education functions and information handling that supports optional or commercial purposes.

Core educational and statutory functions may include:

- enrolment and attendance
- assessment and reporting
- communication with families
- safeguarding and child protection
- student wellbeing and behaviour support
- disability and inclusion planning
- legal and reporting requirements

- continuity of learning
- responding to emergencies and safety risks

These should be differentiated from targeted advertising, commercial profiling, product development, behavioural marketing, training commercial artificial intelligence models, non-essential personalisation and sharing information with unrelated third parties.

The concept of information that is “strictly necessary” may be relatively clear for a simple consumer application but much less straightforward in an educational setting.

Education-specific guidance should provide practical examples showing how the test applies to assessment, intervention, attendance monitoring, learning analytics, wellbeing platforms, communication services and student safety systems.

Withdrawal and destruction of information

The ability to withdraw consent and request destruction of personal information is an important protection. However, these rights must operate consistently with education, safeguarding, public records and legal obligations.

Schools and education authorities may be required to retain information relating to enrolment, attendance, student achievement, incidents and safety, disability adjustments, child protection, complaints, legal proceedings and financial or administrative accountability.

Families may reasonably assume that withdrawal of consent means all information will be immediately deleted. This may not be possible where information has become part of an official school or Department record.

The final Code and supporting guidance should clearly explain:

- what providers must delete
- what information must be retained
- the legal basis for retention
- who remains responsible for retained information
- how information transferred into official records is treated
- what occurs when consent is withdrawn but continued access to the service is educationally necessary

Schools should not be left to explain or resolve these legal distinctions without specialist support.

Artificial intelligence, analytics and automated decision-making

The proposed Code has important implications for the growing use of artificial intelligence and data analytics in education.

The final Code and guidance should explicitly address:

- generative artificial intelligence used by students or staff
- automated assessment and feedback
- adaptive learning platforms
- predictive attendance or engagement analytics
- behaviour and wellbeing risk identification
- facial recognition, voice and image data
- automated decision-making
- the use of student data to train commercial models
- the use of student interactions for product improvement

There should be a clear distinction between information required to provide an educational service and information used to improve or commercialise a provider's product.

Student information should not be used to train general commercial artificial intelligence models without specific, informed and meaningful consent.

Monitoring and online safety

Schools and education authorities use a range of mechanisms to protect students, networks and devices, including web filtering, cybersecurity monitoring, managed device controls, screen and activity monitoring, location-enabled devices, learning activity logs and automated safety alerts.

These functions may be necessary to meet duty of care, online safety and cybersecurity responsibilities.

The final Code should recognise these legitimate purposes while ensuring that monitoring is proportionate, transparent and clearly explained to students in age-appropriate language.

Guidance should distinguish legitimate school safety and security monitoring from commercial tracking, profiling or surveillance.

Procurement and implementation support

Schools do not generally have the legal, technical or privacy expertise to independently assess data architecture, overseas storage and disclosure, subcontracting arrangements, data retention, privacy-by-design settings, cybersecurity controls, artificial intelligence training practices or compliance with consent and deletion requirements.

Implementation should therefore be supported centrally.

The Department should provide:

- an expanded suite of approved products
- clear approval and assurance processes for locally procured services
- standard contractual privacy clauses
- model privacy notices and consent materials
- a common digital consent system
- privacy impact assessment templates
- specialist advice and escalation pathways
- procurement guidance
- staff training
- regular review of approved vendors and services

Local school procurement will continue to be necessary unless the centrally provided suite is significantly expanded. The compliance framework must recognise this reality and support schools accordingly.

Implementation timeframe

The final Code should provide a realistic implementation period.

Schools, education authorities and providers will need time to review existing products and contracts, identify services within scope, redesign privacy and consent processes, adjust platform settings, develop age-appropriate materials, establish deletion and access processes, train staff, communicate with families, resolve legacy data issues and procure replacement services where providers cannot comply.

Implementation should not commence until education-specific guidance, system-level support and approved processes are in place.

Recommendations

SAPPA recommends that the OAIC:

1. Confirm that responsibility for compliance rests primarily with the entity that designs, operates and controls the online service.
2. Clearly distinguish the responsibilities of providers, education departments and individual schools.
3. Confirm that ordinary procurement or use of a third-party service does not make a school or principal the provider of that service.
4. Reconsider the proposed automatic 12-month expiry of consent and provide for consent to remain current where the purpose, data-handling arrangements and risk profile have not materially changed.
5. If annual consent is retained, require it to be centrally coordinated for approved education products rather than separately administered by individual schools.
6. Ensure that students do not lose access to essential educational services solely because a parent or carer has not responded to an annual renewal request.
7. Provide practical arrangements for complex parental responsibility, guardianship and family circumstances.
8. Prevent providers from transferring parental verification and compliance obligations to schools.
9. Clearly distinguish core educational, safeguarding and statutory uses from optional commercial, marketing and product-development uses.
10. Align withdrawal and destruction rights with education recordkeeping, safeguarding and legal obligations.
11. Provide explicit guidance on artificial intelligence, automated assessment, profiling, analytics and the use of student data for product development.
12. Clarify the application of the Code to school device monitoring, web filtering, geolocation and online safety systems.
13. Support Department-level procurement assurance, standard contracts, common consent processes and specialist privacy support.
14. Provide a realistic transition period and ensure education-specific guidance is available before commencement.

SAPPA supports the development of strong and contemporary privacy protections for children. Our comments are intended to assist the OAIC to identify practical implications and possible unintended consequences before the Children's Online Privacy Code is finalised.

Without clearer responsibilities, a more proportionate consent model and strong system-level implementation support, the proposed Code could unintentionally increase school leader workload, disrupt student access to valuable educational services, widen inequity between schools and transfer commercial provider compliance responsibilities to individual public schools.

With appropriate refinement, the final Code could strengthen children's privacy while preserving schools' capacity to select and use digital services that meet the diverse learning, wellbeing and operational needs of their communities.

SAPPA looks forward to further conversation with the OAIC as the proposed Code and supporting guidance are refined.

Thank you,

[redacted]
President
South Australian Primary Principals Association
[redacted]
sappa.com.au
22 June 2026