Government of Western Australia
School Curriculum and Standards Authority

PRIVACY POLICY PRINCIPLES

DOCUMENT INFORMATION	
Responsible officer	Assistant Executive Director, Examination, Certification and Testing
Endorsed	7 April 2026
Reviewed	
Next review date	6 April 2027
CM number	2024/84473[v3]

Acknowledgement of Country

Kaya. The School Curriculum and Standards Authority (the Authority) acknowledges that our offices are on Whadjuk Noongar boodjar and that we deliver our services on the country of many traditional custodians and language groups throughout Western Australia. The Authority acknowledges the traditional custodians throughout Western Australia and their continuing connection to land, waters and community. We offer our respect to Elders past and present.

School Curriculum and Standards Authority
303 Sevenoaks Street
CANNINGTON WA 6107
Further information please contact:
Telephone: +61 8 9273 6300
Facsimile: +61 8 9264 6301
Email: info@scsa.wa.edu.au
Web: www.scsa.wa.edu.au

Document maintenance

This document is to be reviewed and updated as and when required by changing circumstances, with at least one review to be conducted every 24 months. Apart from minor revisions, all revisions to the procedure must be approved and endorsed by the School Curriculum and Standards Authority Board.

Date	Alteration	Rationale	Responsible Officer
7 April 2026	The new Privacy Policy Principles were endorsed by the School Curriculum and Standards Authority Board on 7 April 2026.	Western Australian privacy laws enforcement: *Privacy and Responsible Information Sharing Act 2024*	Principal Consultant, Information Governance

Contents

1. Purpose 1

2. Collection 1

2.1 Why we collect personal information 1

2.2 What personal information we collect 2

2.3 How we collect personal information 2

2.4 Methods of collection 3

2.5 Privacy collection notices 4

3. Use and disclosure 4

3.1 Use and disclosure of personal information 4

3.2 Disclosure outside Australia 5

3.3 Direct marketing 5

3.4 Automated decision-making 6

4. Storage and protection 6

5. Access to and correction of personal information 7

6. Information breach 7

7. Offences under the privacy law 7

8. Communication and awareness 7

9. Contacts 8

10. Appendix 1 Examples of personal information collected and managed by the Authority 9

1. Purpose

The purpose of the *Privacy Policy Principles* (Policy Principles) is to outline how the School Curriculum and Standards Authority (the Authority) collects, manages, uses, and shares personal information in accordance with relevant privacy legislation to fulfil its statutory functions.

The Policy Principles outline the stages of the information privacy lifecycle as follows:

- collection
- use and disclosure
- storage and protection
- access and correction
- incidents and information breaches
- communication and awareness.

These Policy Principles are to be read in conjunction with the Authority's *Privacy Policy* (the Policy) and other relevant privacy laws and authorities outlined in Section 7 of the Policy.

2. Collection

This section outlines how and why the Authority, designated by the *Privacy and Responsible Information Sharing Act 2024* (*PRIS Act*) as an Information Privacy Principle (IPP) entity, collects personal information.

Note: the *PRIS Act* outlines eleven (11) Information Privacy Principles (IPPs) that will be referred to in relevant sections of this document.

2.1 Why we collect personal information

Relevant privacy principles: IPP 1 mandates that personal information collected must be necessary for one or more of the functions or activities of the IPP entity.

Part 3 and Part 3A of the *School Curriculum and Standards Authority Act 1997* (*SCSA Act*) define its functions and powers, outlining the requirements for collecting personal information for specific purposes, including but not limited to:

- registration of students enrolled in the first year of the pre-compulsory or compulsory education in Western Australia (Kindergarten to Year 12)
- enrolment of students according to academic and calendar year into courses, including Australian Tertiary Admission Rank (ATAR) and vocational education and training (VET) units, that result in the Western Australian Certificate of Education (WACE) certification
- enrolment of students into the National Assessment Program – Literacy and Numeracy (NAPLAN) and Online Literacy and Numeracy Assessment (OLNA)
- grading and assessment
- collection of student results and achievement data
- provision of the results of, and reports on, the assessment of student achievements to governing bodies, schools, students, parents and legal guardians of students
- establishment and administration of exhibitions and awards in recognition of student achievement
- conducting and participating in research involving students

- advising the Minister of Education on matters arising under the *SCSA Act*
- communication and engagement with stakeholders.

The Authority also gathers personal information to fulfil its administrative and governance responsibilities in order to facilitate:

- human resource management, including recruitment, employment, and wellbeing services and support
- declaration of conflict of interest
- work health and safety
- financial management, including procurement management
- complaints management
- information access requests
- security
- information and communication technologies provision
- informing policy and strategy
- reporting
- other legal obligations.

The Authority may collect personal information for any other purpose for which consent has been specifically provided (refer to Section 3).

2.2 What personal information we collect

The Authority collects and uses a wide range of personal information to fulfil its role, responsibilities and legal obligations as outlined in Section 2.1.

For example, the Authority holds and maintains personal information such as government-issued student identifiers assigned to students enrolled in primary and secondary education in Western Australia. This is necessary to fulfil its statutory obligations and those of the government. These unique student identifiers are essential for various purposes, including but not limited to student registration, course enrolment, collection of achievement data, access to results and certificates, verification of student eligibility, transfer of student data between jurisdictions, and post-school education and training.

For a comprehensive list of the types of personal information the Authority collects and holds, refer to Appendix 1.

2.3 How we collect personal information

Relevant privacy principles: IPP 1 mandates that the IPP entity gathers personal information solely from the individual unless consent is given for the collection from another source, or collection is required or authorised by or under law, or it is unreasonable or impractical to do so. It also states that personal information must be collected in a fair and reasonable way, and that the purpose for which the information is collected, used, or disclosed must be provided.

2.4 Methods of collection

The Authority collects personal information through the following methods.

Direct collection

The Authority collects personal information from individuals who use its services, sign up for them, or provide services. It does this directly over the phone or through written communications, whether in hard copy or electronic form, including emails, forms, applications, surveys, and online submissions.

Indirect collection

Information, including profile and activity data, may be gathered from digital interactions between the individual and the Authority's online services, such as social media platforms and websites. For information on managing consent for website data collection, refer to the Authority's *Website Privacy Statement*.

Third-party collection

If collecting personal information from an individual is unreasonable, impractical, or required or authorised by or under law, the Authority may obtain information from other sources, such as government bodies, educational institutions and associations, healthcare providers, and parents or legal guardians of minors under sixteen (16) to fulfil its statutory functions (refer to IPP 1 of the *PRIS Act*).

Automated processes

The Authority may collect personal information by automated processes when an individual engages with a process or system, for example:

- audio or visual recordings made for assessment, teaching and training purposes
- surveillance, such as monitoring with CCTV footage that captures images and videos of individuals
- logs of physical access to the Authority's premises using the registration system and security passes
- logs of activities on the Authority's network, devices, information systems and databases.

Unsolicited collection

The Authority might collect personal information without a prior request or direct consent, in the following situations:

- the collection of information is required or authorised by or under law, e.g. the Authority may receive personal information under an Order to Produce
- unsolicited information from third parties, e.g. ministerial correspondence, community petitions
- emergency medical situations, e.g. collecting health information from family members.

2.5 Privacy collection notices

When collecting personal information directly from an individual or indirectly about an individual, the Authority will take reasonable steps to provide a privacy collection notice either before, at the time of, or as soon as practicable after collecting the information. This notice should include the following details:

- the identity of the IPP entity and how to contact it
- the purposes for collecting personal information and how it will be used
- how and with whom the information will be shared
- any law that permits the collection of personal information
- the main consequence (if any) if all or part of the information is not provided
- how the individual can access the personal information that has been collected (refer to Section 9).

The Authority makes all reasonable efforts to ensure that the personal information it collects, uses, or discloses is accurate, complete and relevant.

For more information, refer to the Authority's *Privacy Collection Notice Procedures*.

3. Use and disclosure

This section explains how the Authority uses and discloses personal information.

3.1 Use and disclosure of personal information

Relevant privacy principles: IPP 2 requires that an IPP entity ensure that personal information collected is used and disclosed solely for a specific purpose (the primary purpose) and not used or disclosed for any other purpose unless an exemption listed in IPP 2.1 applies.

Personal information collected by the Authority is used and disclosed for the primary purpose it is collected.

The *SCSA Act*, particularly Part 3A, permits the Authority to disclose student information it collects and manages, to:

- a student, parent, or authorised person, who can request and receive a copy of the student's record, including assessment records, upon payment of a prescribed fee
- contracted service providers to ensure accuracy of student information
- the Minister for Education, who may collect and share information in accordance with the *School Education Act 1999*, including in aggregated form. This information is used for enforcement purposes under the *School Education Act*, such as monitoring, investigating, and ensuring compliance. Additionally, the Minister for Education can share this information with authorised individuals or organisations as necessary for these purposes
- specific entities in aggregated form, such as the Executive Director of Catholic Education Western Australia and the Executive Director of Association of Independent Schools of Western Australia (Inc.), at prescribed times
- research entities, subject to the Authority's Ethics Review Committee's (ERC's) recommendations and the Board's approval, for the purpose of, or in connection with, research involving students.

For details on what information may be disclosed as part of the research application, refer to the Authority's *Research Governance Policy and Policy Principles*.

The Authority may also disclose personal information for a related secondary purpose where one of the following applies, as outlined in IPP 2.1 of the *PRIS Act*:

- it is reasonable for it to be expected in line with the primary purpose
- with the consent of an individual or authorised representative/s, e.g. transfer of student records interstate upon receiving a notice of transfer with parental or guardian consent (regulated by the *Interstate Student Data Transfer Note (ISDTN) and Protocol)*
- when the Authority reasonably believes it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual, public health, public safety or public welfare or a threat to any individual due to family violence
- when required or authorised by or under legislation or court/tribunal order, e.g. the *Freedom of Information Act 1992* (FOI Act) or the *Criminal Investigation Act 2006*
- to investigate or report suspected unlawful activity, or when reasonably necessary for a specified law enforcement purpose, including the prevention or investigation of a criminal offence or seriously improper conduct, by or on behalf of a law enforcement agency
- as de-identified information for research or statistics purposes, or to inform the agency's policy and strategy
- to establish or respond to a legal claim.

3.2 Disclosure outside Australia

Relevant privacy principles: IPP 9 states that disclosing personal information relating to an individual to a person (other than the individual) outside Australia is not permitted unless certain exemptions apply. IPP 9 also mandates that personal information disclosed outside Australia must be protected from misuse, loss, or unauthorised re-identification, access, modification, or disclosure.

The IPP 9.1 of the *PRIS Act* outlines the conditions under which information can be disclosed outside Australia. Specifically, the Authority is permitted to share personal information about overseas students with educational institutions outside Australia that offer the Western Australian Curriculum in which these students are registered. This disclosure is necessary to fulfil the Authority's legal and contractual obligations. Additionally, the Authority adheres to the requirements of IPP 9.2 and implements appropriate data protection measures to ensure that this information is safeguarded against misuse, loss, and unauthorised access.

3.3 Direct marketing

The Authority does not use or disclose personal information for direct marketing purposes unless it has obtained the required consent as per IPP 2. The Authority takes reasonable steps to respond to requests to opt out of receiving direct marketing communications and to disclose the source of the information. These requests will be handled within a reasonable timeframe, and confirmation will be provided once the request has been completed.

3.4 Automated decision-making

Relevant privacy principles: IPP 10 states that an IPP entity that employs an automated decision-making process involving the use of personal information to make a significant decision about an individual must conduct a privacy impact assessment and periodically evaluate the effectiveness of that process. It also states that the individual must be notified that an automated decision-making process was employed, and be provided a process by which the individual can request human intervention in relation to the decision.

When the Authority employs any automated decision-making process involving personal information when significant decisions about individuals are made, the Authority will make an assessment evaluate privacy risks related to the use and handling of personal information. This assessment may be a privacy impact assessment (PIA). The Authority will also inform affected individuals that the decision was automated and, if requested, provide details on how the automated decision was made. Furthermore, when the Authority notifies individuals that a decision about them was made by an automated process, it will provide instructions on how to request a human review of that decision, should they request this.

4. Storage and protection

Relevant privacy principles: IPP 4 requires that an IPP entity takes reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification, or disclosure. Personal information that is no longer needed for any purpose, unless the IPP entity is expressly required or authorised to retain the information by or under another law, must be destroyed or permanently de-identified.

The Authority takes all reasonable steps to protect personal information from misuse, loss, unauthorised access, modification, and disclosure in accordance with the departmental *Cybersecurity Policy*, which aligns with the *Australian Cyber Security Centre (ACSC) Essential Eight* requirements and other privacy laws.

One of the measures the Authority employs to protect personal information and to minimise privacy risks is the de-identification of data used for research, reporting, and statistical purposes. The Authority makes every effort to comply with IPP 11 of the *PRIS Act*, ensuring that de-identified information cannot be re-identified, accessed, modified, or disclosed unless authorised by or under law. This involves establishing internal procedures for de-identifying data and following the internal decision-making and approval processes for releasing information.

The management of electronic and physical records, including their access, storage, and disposal, is consistent with the Authority's *Recordkeeping Plan* (RKP) and *Records Management Policy and Procedures* and aligned with the *State Records Act 2000* (*SRO Act*) and the *State Records Principles and Standards 2002*.

5. Access to and correction of personal information

Relevant privacy principles: IPP 6 mandates that an IPP entity must provide an individual with access to their personal information upon request, provided that doing so does not pose a risk to anyone's safety or any other reasons detailed in IPP 6.1 of the *PRIS Act*.

A person or their authorised representative/s can access their personal information held by the Authority by submitting a written request. This can be done informally or through a Freedom of Information (FOI) request under the *Freedom of Information Act 1992 (FOI Act)* and in compliance with IPP 6 and Division 4 of the PRIS Act. The FOI request must specify which records the applicant wants to view and include a valid Australian address for the response. Additionally, the individual may request corrections to any information about themselves that is incomplete, incorrect, or misleading.

For instructions on how to submit an FOI request for access to, or correction of, personal information, see Section 9.

6. Information breach

Relevant privacy provisions: Division 6, s. 57 of the *PRIS Act* states that a notifiable information breach occurs when there is unauthorised access to, disclosure of, or loss of personal information held by an IPP entity, which is likely to result in serious harm to any individual to whom the information relates.

If an information breach is suspected or known to have occurred, the Authority's *Information Breach Policy* takes effect. This policy has been developed to meet the requirements of the mandatory information breach notification scheme under Division 6 of the *PRIS Act*.

Breaches related to research data are managed in accordance with the Authority's *Research Governance Policy and Policy Principles*.

Cybersecurity incidents are managed in accordance with the departmental *Cybersecurity Policy*.

7. Offences under the privacy law

The risks of noncompliance with the *PRIS Act* provisions are substantial and may negatively impact the Authority's reputation, potentially resulting in penalties. These may include, but are not limited to:

- fines of up to $60,000 issued to the IPP entity for not complying with the Information Commissioner of Western Australia's compliance notices
- compensation orders of up to $75,000 for an eligible privacy complaint lodged by the affected individuals
- potential imprisonment of up to three years for individuals who breach *PRIS Act* obligations.

8. Communication and awareness

The Authority provides information to individuals in the following ways:

- by making the Policy and the Policy Principles accessible on the Authority website
- through privacy collection notices and consent forms, as outlined in Section 2.

To assist staff with privacy-related matters, the Authority:

- publishes privacy-related policies, procedures, and guidance on the Authority's intranet
- conducts privacy induction programs
- offers online privacy training
- provides guidance and support from the Authority's Information Governance team when specific privacy requirements need to be addressed.

9. Contacts

The Authority respects individuals' rights to remain anonymous or use a pseudonym when engaging with us, provided it is lawful and practical to do so.

Access and amendment of personal information

To lodge an FOI request for access to, or correction of, personal information, individuals should refer to the Authority's *Public Information Statement* available on the Authority website. The FOI request or enquiries are directed to FOI@scsa.wa.edu.au.

Inquiries

Privacy inquiries regarding the Authority's management of personal information should be directed to the Authority's Information Governance team at privacy@scsa.wa.edu.au.

Complaints

Individuals can submit a privacy complaint to the Authority at privacy@scsa.wa.edu.au. The Authority handles complaints according to the departmental *Complaints and Notifications Policy*. Individuals can also file a complaint directly with the Office of the Information Commissioner of WA (OIC WA) for a violation of the *PRIS Act* via info@oic.wa.gov.au.

Additional information about privacy is available on the OIC WA's website.

10. Appendix 1 Examples of personal information collected and managed by the Authority

Categories	Types of personal information collected may include, but are not limited to:
Students	• Student details: photograph, contact details, address, date of birth, place of birth, unique student identifier, language spoken, previous education, subjects, courses, qualifications attained, fee payment, visa and immigration status. • Sensitive personal information relating to ethnicity, Indigenous status, and gender identity. • Student permission forms, e.g. to use their schoolwork, and examination responses (written and practical), to create educational resources and for media communications to publish details of the award winners. • Special consideration requests, which may include health information if relevant, e.g. aquitable access adjustments • Leave of absence for examinations and testing. • Assessment and examination records, including marks, progress reports, comments, final grades and certification. • Graduation records, including receipt of prizes, awards, and scholarships. • Reports of hazards and incidents during the examinations and testing periods, which may include health information. • Complaints, misconduct, and appeals, and resulting outcomes, including any investigations. This may involve health information or sensitive personal details, as applicable. • Completion of mandatory or optional training. • Health information related to disabilities and/or accessibility needs, medical history in some cases, e.g. evidence of vaccinations, where relevant. Health information may also be relevant to special considerations, leave of absence or withdrawal requests.
Parents/guardians	• Parents/guardians details: contact details, address, date of birth, place of birth, language spoken, completed education, parental consent.
Teaching and learning	• Comments and personal details provided in survey responses. • Assessments and coursework of students and/or created by teachers.

Categories	Types of personal information collected may include, but are not limited to:
Research	• Research management-related records such as Ethics Review Committee minutes, participant consent and information forms, intellectual property agreements and licences, and grant applications, if applicable. • Data collected and disclosed as part of approved research activities, which may include personal information, sensitive personal information or health information, depending on the research.
Staff	• Recruitment information relating to potential candidates, as well as applicants, including contact details, applications, CVs, candidate databases (which may include salary information), previous employment details, referee reports, skills assessments, psychometric and personality profiles, interview records, working with children checks, criminal background checks, and qualification checks for academic credentials. • Eligibility to work in Australia checks, including visa information and information collected in relation to sponsored visas. • Staff details: date of birth, photograph, unique employee identifier, contact details, address, emergency contact details, tax declarations, banking details, contracts of employment, previous employment details, salary details, superannuation information, training undertaken and results, if applicable, changes in the contract, including work arrangements, acting roles, promotions, including applications, CVs, qualifications, referee reports, references, code of conduct and conflicts of interest. • Sensitive personal information relating to ethnicity, Indigenous status, gender identity or trade union membership, if applicable. • Leave requests, approvals and related documents. This may include health information for some types of leave, such as personal leave. • Work planning and performance reviews, including comprehensive assessment reports, probation plans and performance management. • Reports of hazards and incidents, which may include health information. • Grievances, complaints and misconduct, appeals and resulting outcomes, including any investigation. This may include health information or sensitive personal information, as applicable. • Personal information relevant to warrants, court orders, subpoenas, contracts or other legal matters. • Completion of mandatory or optional training.

Categories	Types of personal information collected may include, but are not limited to:
	• Health information relating to workers' compensation, accidents and injury-related information, medical certificates, health reports and questionnaires. • Resignations or retirements, or other forms of separation, including exit interviews. • Personal details of nominated, appointed and elected committee members. • Medical records, including personal details, confidential health information or sensitive personal information required for the provision of services, such as health or counselling services. • Wellbeing services and support, e.g. the Employee Assistance Program (EAP) or health case management.
Community and industry engagement and partnership	• Philanthropy activities, including history, dates, and contact details. • Gift acceptance details, e.g. donor details. • Names and contact details of prospective partners, e.g. overseas associates. • Names and contact details of volunteers. • Event management, including attendee information, such as contact details, titles, position details, dietary and access requirements. This may include relevant health information of the event attendees. • Community surveys and consultations regarding the Authority's activities.
Administrative activities	• Financial details, such as creditors, debtors and bank account details. • Declarations of conflicts of interest. • Protected disclosures. • Information access requests, such as under the *FOI Act* or other privacy laws. • Access logs and audit trails of staff activity using information systems, technologies, and physical locations. • Administrative records dealing with governance, finance, property, building security, and procurement. • Information and communication technologies records, such as email and other account information, websites and cookies.

Source: Adopted from University of Technology Sydney. (2021). *UTS Privacy Management Plan*. University of Technology Sydney, Sydney.