Āura EDUCATION

PRIVACY

POLICY AND PROCEDURE



Status: Current

Version: 2.0

Effective Date: 11 August 2026

1. Rationale and policy statement

Rationale

Aura Education considers the protection of personal information to be fundamental to the trust students place in the college. It collects personal information in order to enrol students, deliver and assess their training, provide support, and meet the reporting obligations that apply to a registered training organisation and a CRICOS provider.

A significant proportion of this information is sensitive, and certain records must be retained for thirty years. Students have limited ability to withhold it, and responsibility for its proper handling therefore rests entirely with Aura Education. By collecting only what is required, protecting it appropriately, and being transparent about its use, the college aims to meet its obligations under the Privacy Act 1988 and to maintain the confidence that allows students to disclose a disability, a support need or a complaint.

Policy statement

Aura Education will:

- collect only the personal information it needs for a lawful purpose connected to its functions, and tell each individual what is collected, why, and who it will be given to;
- use and disclose it only for that purpose, a directly related purpose the person would reasonably expect, or where the law requires it;
- take reasonable technical and organisational steps to protect it from misuse, interference, loss and unauthorised access, modification or disclosure;
- give individuals access to their own personal information, and correct it when it is wrong;
- retain records for as long as the law requires and destroy or de-identify them securely when that period ends;
- respond to a suspected data breach promptly, and notify affected individuals and the Office of the Australian Information Commissioner where the law requires it;
- disclose any use of automated decision-making that significantly affects a person's rights or interests; and
- deal with privacy complaints fairly and without detriment to the person who raises them.

2. Definitions

Term	Meaning
APPs	The thirteen Australian Privacy Principles in Schedule 1 to the Privacy Act 1988 (Cth), which govern how personal information is collected, used, disclosed, secured, accessed and corrected.

Term	Meaning
Automated decision making	A decision made, or substantially and directly assisted, by a computer program using personal information, where the decision could reasonably be expected to significantly affect a person's rights or interests.
Consent	Voluntary, informed, current and specific agreement to the collection, use or disclosure of personal information. Consent is not assumed from silence and may be withdrawn.
Eligible data breach	Unauthorised access to, or disclosure of, personal information, or its loss in circumstances where unauthorised access or disclosure is likely, that is likely to result in serious harm to any person the information relates to.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.
Sensitive information	A subset of personal information including health information, disability, racial or ethnic origin, religious or philosophical beliefs, political opinions, sexual orientation, criminal record, and biometric information. It attracts a higher level of protection.
Serious harm	Not defined in the Privacy Act. In the context of a data breach it may include serious physical, psychological, emotional, financial or reputational harm.
USI	The Unique Student Identifier issued under the Student Identifiers Act 2014 (Cth), which every student undertaking nationally recognised training must have.

3. Purpose

This document explains what personal information Aura Education holds, why it holds it, and how it is protected. It covers:

- what is collected and from whom, and what people are told at the point of collection;
- when personal information may be used or disclosed, and to whom;
- how information is stored, secured, retained and destroyed;
- how a person accesses or corrects their own information;
- what happens when a data breach is suspected; and
- who does what, and what has to be recorded.

4. Scope

This document applies to all personal information Aura Education collects, holds, uses or discloses about prospective, current and former students, staff, contractors, education agents, employers and any other individual, in electronic or physical form, whether held on Aura Education premises or hosted externally on its behalf.

It applies to all staff, trainers, assessors, contractors, education agents and third parties who handle that information.

5. Alignment and legislative context

Type	Instrument	Relevance
Legislation	Privacy Act 1988 (Cth) and the Australian Privacy Principles	The primary obligation. Governs collection, notice, use, disclosure, security, retention, access and correction, and establishes the Notifiable Data Breaches scheme.
Legislation	Privacy and Other Legislation Amendment Act 2024 (Cth)	Introduced a tiered civil penalty regime and expanded regulator powers, a statutory tort for serious invasions of privacy in force since 10 June 2025, criminal offences for doxxing, and new automated decision-making transparency requirements in APP 1.7 to 1.9 which take effect on 10 December 2026.
Legislation	Student Identifiers Act 2014 (Cth) and Regulations	Govern the collection, verification, use and disclosure of a student's USI, and restrict the purposes for which it may be used.
Legislation	Education Services for Overseas Students Act 2000 (Cth) and the National Code of Practice 2018	Require the collection and reporting of overseas student information through PRISMS, including course progress, attendance and changes to enrolment, and permit disclosure to the Department of Home Affairs, the Tuition Protection Service and the Overseas Students Ombudsman.
Legislation	National Vocational Education and Training Regulator Act 2011 (Cth)	Requires student and training records to be created, retained and made available to the regulator.
Standard	Outcome Standards for NVR Registered Training Organisations 2025	Standard 2.1 requires students to be given clear and current information about the organisation and its services. Standards 4.1 and 4.4 require integrity in operations and monitoring and continuous improvement of them. Records obligations sit under the Compliance Standards instrument.
Guidance	OAIC Australian Privacy Principles Guidelines, and the OAIC Data Breach Preparation and Response Guide	How the regulator interprets each APP, and the four-step containment, assessment, notification and review process applied in Procedure 8.6.
Guidance	National VET Data Policy and AVETMISS reporting requirements	Set out what student data must be reported, to whom, and the privacy notice students must be given at enrolment.

6. Staff responsible

Role	Responsibilities
Chief Executive Officer (CEO)/ Compliance	Approves this document, decides whether a data breach is notifiable, and is accountable for privacy compliance. Maintains this document and the records that support it, receives and acts on suspected breaches, manages privacy complaints and access requests, and reports.
Admissions Officer	Collects personal information at application and enrolment, gives the collection notice, obtains consent and verifies the USI.
Trainers, assessors and support staff	Collect and record only what is needed, keep student information secure and confidential, and report a suspected breach immediately.
IT / systems support	Maintains system access controls, individual accounts, backups and security measures, and assists with containment when a breach occurs.
Education agents and third parties	Handle personal information in accordance with their written agreement with Aura Education and to a standard no lower than this document.
All staff	Read, understand and apply this document, and raise any privacy concern or suspected breach with the CEO/Compliance without delay.

7. Breach of policy

A breach of this document includes collecting more information than is needed, using or disclosing personal information for a purpose the person did not agree to and the law does not permit, leaving records where others can see them, sharing account credentials or sending personal information to the wrong recipient, failing to report a suspected data breach, and accessing a student's or colleague's record without a work reason to do so.

Breaches are investigated by the CEO/Compliance and managed under the Complaints and Appeals Policy and Procedures. The person concerned is told the substance of the allegation and given an opportunity to respond before a finding is made, and the decision, reasons and outcome are recorded. Consequences may include additional training, corrective action, disciplinary action, or termination of a third-party or agent agreement.

A person may also complain directly to the Office of the Australian Information Commissioner. Nothing in this document limits that right, and no person is disadvantaged for exercising it.

8. Procedures

8.1 Collecting personal information

Responsibility: Admissions Officer; all staff

1. Collect only the personal information reasonably necessary for enrolment, training, assessment, support, reporting or a related function. This includes name, contact details, date of birth, gender, country of birth, citizenship or visa details, language spoken at home, prior education, employment, USI, and where relevant disability, language, literacy, numeracy and digital literacy needs and assessment outcomes.
2. Collect personal information directly from the individual wherever possible. Collect it from an education agent, employer or another party only where the individual has asked for this or has consented.
3. Collect sensitive information only where the individual consents and it is reasonably necessary, or where the law requires or authorises it.
4. Where a person objects to providing background information, accommodate the objection where possible, but obtain enough detail to identify the person and to obtain and verify their USI. Certification cannot be issued without a verified USI unless the USI Registrar has granted an exemption.
5. Assess any unsolicited personal information within a reasonable period, and destroy or de-identify it if it could not lawfully have been collected.

8.2 Telling people what is collected and why

Responsibility: Admissions Officer

1. Give every applicant a collection notice at or before the time of collection, through the enrolment form, the student handbook and the website, stating who Aura Education is and how to make contact, what is collected and why, who the information will be disclosed to, the law requiring its collection, how to access or correct it, how to complain, and the consequences of not providing it.
2. Include in the enrolment form the privacy notice required by the National VET Data Policy, and obtain the student's signature confirming they have read it and authorising verification of their USI.
3. Obtain separate written consent before disclosing information to a parent, employer, agent or any other third party, and record that consent on the student file.
4. Tell students that consent may be withdrawn, and record any withdrawal.

8.3 Using and disclosing personal information

Responsibility: All staff

1. Use personal information only for the purpose it was collected for, a directly related purpose the person would reasonably expect, or a purpose the person has consented to.
2. Disclose personal information outside Aura Education only where the law requires or authorises it, or the person has consented. Disclosures required by law include reporting to the National VET Regulator, NCVER, the USI Registrar, the Department of Home Affairs through PRISMS, the Tuition Protection Service, and Commonwealth, state or territory funding agencies.
3. Refer any request for information about a student from a person or body outside Aura Education to the CEO/Compliance before responding.

4. Do not use or disclose personal information for direct marketing without consent, and act on any request to opt out.
5. Record each disclosure made outside the ordinary reporting obligations, including what was disclosed, to whom, when, and on what basis.
6. Ensure every education agent and third party that handles personal information on Aura Education's behalf is bound by a written agreement requiring a standard of protection no lower than this document.

8.4 Storing, securing, retaining and destroying information

Responsibility: IT / systems support; Finance/Record keeper/ Compliance

1. Store electronic records in Aura Education's student management system and approved systems, protected by individual user accounts, access limited to staff who need it for their role, current security software and regular backups. Accounts are not shared. Review access rights at least annually, and remove access when a person changes or leaves a role.
2. Store hard copy records in locked storage, accessible only to authorised staff, and do not remove student files from Aura Education premises without the CEO's approval.
3. Do not send personal information to a personal email address or store it on a personal device or unapproved cloud service.
4. Retain student and training records for the period required by law, including the retention of records required for the issuing of qualifications and statements of attainment, and retain overseas student records for the period required under the ESOS framework.
5. Destroy or securely de-identify personal information once the retention period has ended and it is no longer needed for any lawful purpose, and record what was destroyed and when.

8.5 Access and correction

Responsibility: CEO

1. Accept a request for access or correction in writing, including by email, and acknowledge it on receipt.
2. Verify the identity of the person making the request before releasing anything.
3. Respond within a reasonable period and at no charge. Where access is refused, give written reasons and explain how to complain.
4. Correct information shown to be inaccurate, out of date, incomplete or misleading, confirm the correction to the person, and notify any third party that was given the incorrect information.
5. Record every request, the response and the outcome.

8.6 Responding to a data breach

Responsibility: All staff to report; CEO/Compliance to act

1. Any staff member who suspects personal information has been lost, accessed, disclosed or altered without authorisation reports it to the CEO/Compliance immediately. Reporting a suspected breach is not itself a breach of this document.

2. **Contain:** Take immediate steps to limit further access or disclosure, such as disabling an account, recovering a device or recalling a message.
3. **Assess:** Establish what happened, whose information is involved, and whether serious harm is likely. Complete the assessment expeditiously and within thirty days, and document the reasons if that is not possible.
4. **Remediate:** Take action to reduce the risk of harm. If remedial action makes serious harm unlikely, notification is not required and the matter proceeds to review.
5. **Notify:** Where serious harm remains likely, the breach is an eligible data breach. The CEO notifies the Office of the Australian Information Commissioner using its online form, and notifies the affected individuals, telling them what happened, what information was involved, and what steps they should take.
6. **Review:** Investigate the cause, decide what will prevent a recurrence, and record the incident, the decisions and the actions in the register.
7. Consider whether the incident should also be reported to police, the Australian Cyber Security Centre, ASQA or another body.

8.7 Automated decisions

Responsibility: CEO/ Compliance

1. Maintain a record of any computer program used to make, or substantially and directly assist in making, a decision that could significantly affect a person's rights or interests, including the kinds of personal information used and the types of decisions involved.
2. Disclose that information in this document before 10 December 2026, when the requirement in APP 1.7 to 1.9 takes effect.
3. At the date of this version, Aura Education does not use automated decision-making to make decisions that could significantly affect a person's rights or interests. The ACER Core Skills Profile automatically scores a prospective student's responses, but the score is one input to advice given by a member of staff, who makes the decision on suitability. This position covers the pre-enrolment assessment and Aura Education's student management system and is reviewed if either changes or a new system is introduced.

8.8 Monitoring, records and review

Responsibility: CEO/Compliance

1. Maintain a register of privacy complaints, access and correction requests, data breaches and disclosures made outside routine reporting.
2. Include privacy in staff induction and in the annual professional development plan, covering collection notices, secure handling, and how to report a suspected breach.
3. Report privacy complaints, breaches and trends to the CEO at least annually, and record each improvement in the Continuous Improvement Register with an owner and due date.
4. Review this document annually, or earlier following a change to privacy legislation, a data breach, a substantiated complaint, or a significant change to Aura Education's systems.

9. Related documents

Policies and procedures: Complaints and Appeals Policy and Procedures; Enrolment Policy and Procedure; Attendance Monitoring Policy and Procedure; Student Support Policy and Procedure; Deferral, Suspension and Cancellation Policy and Procedures; Digital Literacy Policy and Procedure; Diversity and Inclusion Policy and Procedures.

Forms and registers: Aura Education enrolment form; Complaints and Appeals Register; Continuous Improvement Register.

10. Version control

Version	Date	Author	Approved by	Change description
2.0	11 August 2026	Compliance	CEO	Reviewed and Updated for the Privacy and Other Legislation Amendment Act 2024, including the automated decision-making transparency requirement commencing 10 December 2026. Procedures added for collection, use and disclosure, storage and retention, access and correction, and data breach response.
1.0	11 November 2024	Compliance	CEO	Original policy