

06. Privacy, Confidentiality and Data Retention Policy and Procedure

Document Name	06. Privacy, Confidentiality and Data Retention P&P 2025_v1.3
Status	Approved
Approved By	Tim Koster
Approval Date	21/08/2025
Review Date	21/08/2027
Standard Reference	Compliance Requirement 20 Privacy Act 1988 (Cth), including the: • Australian Privacy Principles (APPs) • Student Identifiers Act 2014 (Cth) • Fair Work Act 2009 (Cth) • Records Services requirements under the Standards for RTOs 2025 • Electronic Transactions Act 1999 (Cth) • South Australian Information Privacy Principles (IPPs) (where applicable)
Signature	

Table of Contents

Policy	3
Definitions	3
Procedure.....	4
1. Collection of Personal Information	4
2. Use and Disclosure of Personal Information	4
3. Access and Correction	4
4. Security of Data	4
5. Data Retention and Disposal.....	4
6. Staff Responsibilities and Training	5
Extracts from Standards	6

06. Privacy, Confidentiality and Data Retention Policy and Procedure

Policy

Minda Inc t/a South Australian Learning Centre (SALC) is committed to protecting the privacy and confidentiality of all personal, sensitive and training-related information it collects and holds. The organisation complies with all applicable Commonwealth, State and Territory legislation relating to the handling, storage and disclosure of information, including but not limited to:

- Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs)
- Student Identifiers Act 2014 (Cth)
- Fair Work Act 2009 (Cth)
- Records Services requirements under the Standards for RTOs 2025
- Electronic Transactions Act 1999 (Cth)
- South Australian Information Privacy Principles (IPPs) (where applicable)

All personal information, including USI records, student files, enrolment data, assessment evidence and communications, is handled in a secure and lawful manner. Data is collected only for legitimate operational and compliance purposes and individuals are informed of the reasons for collection and their rights under privacy legislation.

SALC ensures that data is retained, archived and disposed of in accordance with applicable regulatory and contractual requirements, including VET data reporting obligations, audit readiness and funding agreements. Access to confidential information is restricted to authorised personnel and systems are in place to prevent unauthorised access, alteration, or loss.

Definitions

Term	Definition
Personal Information	Any information or opinion about an individual who is identified or reasonably identifiable. This includes names, addresses, contact details, academic records, and USI data.
Sensitive Information	A subset of personal information that includes data about a person's health, disability, ethnicity, religious beliefs, criminal record, or membership of a trade union.
Australian Privacy Principles (APPs)	A set of 13 principles under the Privacy Act 1988 that govern the collection, use, storage, and disclosure of personal information by Australian organisations.
Student Identifiers Act 2014	Commonwealth legislation that governs the use, protection, and verification of Unique Student Identifiers (USIs) in the VET sector.
Confidentiality	The ethical and legal obligation to protect personal or sensitive information from being disclosed to unauthorised persons.
Data Retention	The practice of storing data for a defined period to meet legal, regulatory, or operational requirements.

Procedure

1. Collection of Personal Information

- 1.1. Information is collected directly from students, staff, employers or third parties only when it is required for the delivery of training and assessment services or to meet legislative obligations.
- 1.2. Students and staff are informed at the time of collection about the purpose of data collection, how their data will be used and their rights under the Privacy Act.
- 1.3. Consent is obtained where required, particularly for the collection of sensitive information or for sharing data with external parties.

2. Use and Disclosure of Personal Information

- 2.1. Personal information is only used for its intended purpose or a directly related secondary purpose that the individual would reasonably expect.
- 2.2. Data is disclosed to third parties (e.g. regulators, funding bodies, auditors, NCVER) only when required by law or when explicit consent has been provided.
- 2.3. Unique Student Identifier (USI) records are accessed and stored in accordance with the Student Identifiers Act 2014, and access is limited to authorised staff.

3. Access and Correction

- 3.1. Individuals have the right to request access to the personal information held about them and to request corrections where they believe the information is inaccurate or incomplete.
- 3.2. Requests must be submitted in writing and will be processed within a reasonable timeframe. Verification of identity will be required prior to release of any information.

4. Security of Data

- 4.1. All digital student records are stored on secure systems with role-based access controls and password protection.
- 4.2. Paper records are kept in locked storage and only accessible by authorised staff.
- 4.3. Data breaches or unauthorised access incidents are reported and managed in accordance with the Notifiable Data Breach Scheme under the Privacy Act, where applicable.

5. Data Retention and Disposal

- 5.1. Records are retained for the minimum periods set out under the Standards for RTOs and other applicable laws, including:

06. Privacy, Confidentiality and Data Retention Policy and Procedure

- **Records of AQF certification documentation issued:** 30 years
- **Completed student assessment items and evidence:** minimum 2 years after the learner completes the training product
 - **However,** According to our FAA with Skills SA, we are required to keep assessment evidence indefinitely.
- **Financial and accounting records:** 7 years, in accordance with Australian taxation and corporate record-keeping requirements

5.2. Disposal is conducted by authorised personnel or contractors under formal arrangements.

6. Staff Responsibilities and Training

6.1. All staff are required to comply with this policy and are trained on privacy, confidentiality and data handling obligations as part of their induction.

6.2. Staff found to have breached confidentiality or data security will be subject to disciplinary action, up to and including termination of employment.

Extracts from Standards

Compliance Requirement 20 - Compliance with Laws

An NVR registered training organisation must comply with all applicable Commonwealth, State and Territory laws, including, for example, by ensuring:

- a personal information is collected, used and disclosed by the organisation in accordance with all applicable privacy laws; and
- b the organisation complies with all applicable requirements under the Student Identifiers Act 2014.

Note There are a range of laws that may be applicable under this section. The examples provided in paragraphs (a) and (b) are for illustrative purposes.