

Privacy Policy

1. Purpose

Purpose of the Policy to ensure responsible management and protection of personal information in line with privacy principles.

- Ensures PICAC manages personal information responsibly.
- Maintains privacy, confidentiality, and security of data related to students, staff, employers, and third parties.
- Clearly outlines how personal information is collected, used, stored, and accessed.
- Ensures individuals understand their rights regarding their personal data.

2. Scope

This policy applies to all personal information collected, used, stored, or disclosed by PICAC relating to students, staff, contractors and third parties, industry partners and employers, and any other stakeholders interacting with PICAC's training and assessment services.

3. Standards Referenced

Standards for RTOs 2025:

Outcome Standards 2025 - NA

Compliance Standards 2025:

- Part 2- Division 3 – Standard 20(a) – Compliance with Laws.

4. Policy Statement

PICAC is committed to protecting personal information in line with legislative and regulatory requirements.

- Ensures compliance with the Privacy Act 1988, Australian Privacy Principles, and Standards for RTOs 2025.
- Maintains the privacy, confidentiality, and security of personal data relating to students, staff, employers, and third parties.
- Ensures individuals are informed of their rights to access and correct their personal information.

5. Legislative and Regulatory Framework

PICAC complies with:

- Privacy Act 1988
- Australian Privacy Principles
- Relevant state-based privacy laws
- Applicable funding contract conditions
- SRTOs 2025

The APPs are grouped into:

- Part 1 – Consideration of personal information privacy
- Part 2 – Collection of personal information
- Part 3 – Dealing with personal information.
- Part 4 – Integrity of personal information
- Part 5 – Access to, and correction of, personal information

6. Privacy Commitment

PICAC is committed to protecting the privacy and confidentiality of personal and sensitive information through the following principles:

- Collection: Only collect information necessary for our functions and only with informed consent.
- Use: Personal information only for the purpose for which it was collected.
- Disclosure: Never disclose or share personal information without written consent unless required by law.
- Protection: Securely store data and protect against misuse, loss, or unauthorised access.
- Transparency: Clearly inform individuals of their rights to access and correct their information.
- Regulatory Reporting: Fulfil obligations for reporting, funding, and regulatory requirements with respect to information privacy.

7. Types of Information Collected and Stored

Students

- Full name, date of birth, contact details.
- USI, student identifiers, concession details
- Residency/citizenship information
- Disability, medical or learning support needs.
- Assessment records and progress
- Transcripts and RPL/Credit Transfer documents
- Employer feedback (where applicable)

Staff

- Personnel files (e.g., employment contracts, qualifications)

Employers and Third Parties

- Contact details
- Information provided for funded training delivery.

All records are managed through secure systems such as VETtrak and are password-protected. Access is role-based and limited to authorised personnel only.

8. Data Breach Notification

If a suspected or actual data breach occurs:

- The CEO must notify relevant government departments or funding bodies as soon as practicable.
- PICAC will assess and manage the breach in accordance with the Notifiable Data Breaches (NDB) scheme under the Privacy Act.

9. Accessing and Correcting Personal Information

Any individual may request access to the personal information PICAC holds about them by:

- Submitting a written request identifying the information sought
- Providing proof of identity

Corrections can be requested in writing. PICAC will take reasonable steps to ensure that personal information is accurate, complete, and up to date.

10. Website Privacy

PICAC's website may contain links to external websites. PICAC is not responsible for the privacy practices of these websites. Users are advised to consult the privacy statements of external sites before providing personal information.

11. Use of Personal Information

Personal information may be used to:

- Provide course information and support.
- Manage enrolment, delivery, and administration of training.
- Verify USIs and eligibility for funding.
- Maintain accurate academic records.
- Report to regulatory and government bodies as required.
- Issue media releases or promotional materials that include personal information (e.g., name, image, testimonial) only with the individual's prior written consent, in accordance with PICAC's Privacy and Marketing Policies.

Failure to provide requested personal information may result in PICAC being unable to enrol or support the individual.

12. Supporting Processes

Process Name	Purpose
PRO_RTOManagement_V1	Processes and Procedures
FC39_RequestingAccessstoPersonalInformation_V2.2	Request for Student Information

13. Supporting Documents

Document ID	Name
FORM_Pre-TrainingInterviewRecord_V2.2	Pre-Training Interview Record
Code of Conduct Agreement(TBD)	Code of Conduct Agreement

14. Version Control

Version	Date	Change Summary
1.0	27/10/2017	Initial release
1.1	29/08/2018	Updated forms and document references
2.0	03/06/2024	Policy review and realignment with SRTOs 2015
2.1	23/05/2025	Comprehensive revision; aligned to 2025 SRTOs updates
2.2	01/09/2025	The logo has been updated to include PICAC, STC, CEPUTEC, and FIT.
2.3	13/01/2026	The SRTO 2015 reference has been removed.

15. Summary of Changes:

Category	Change Type	Summary
Structure	Revised	Simplified layout with clear sections and headings.
Standards Referenced	Updated	Now includes SRTOs 2025 (Standard 20(a)).
Legislative Scope	Expanded	Added state privacy laws and funding contract obligations.
Privacy Commitments	Refined	Clear principles for collection, use, disclosure, and access.
Data Types	Clarified	Information grouped by stakeholder (students, staff, third parties).
Data Breach Response	New Section	Includes Notifiable Data Breaches (NDB) process.
Access & Corrections	Clarified	Sets out process to request or correct personal information.
Supporting Materials	Updated	Aligned forms, processes, and document IDs.