

PRIVACY & DATA SECURITY POLICY

Document Title	Privacy & Data Security Policy
Approval Date	12/01/2026
Next Review Date	12/01/2027 or following a significant change
Applies To	All staff, contractors, trainers, assessors and third parties who handle student or staff personal information; all students, participants and prospective students

Document History

Version	Date	Summary of Change	Approved By
1.0	12/01/2026	Merged with the detailed ASQA 2025-aligned Privacy Policy; added Outcome/Compliance/Credential Policy alignment, identity & access controls, and evidence integrity sections.	Compliance

1. Purpose

Asuria People Services Pty Ltd ("Asuria", "we", "us", "our") holds a lot of personal information about our students, participants and staff — names, contact details, Unique Student Identifiers (USIs), results, and sometimes health, identity or financial information. People trust us to look after that information properly.

This Policy explains, in plain and professional language, what personal information we collect, why we collect it, how we keep it safe, how long we keep it, and what rights individuals have over their own information. It also sets out how our privacy, information security and record-keeping practices support the quality and integrity outcomes required of Registered Training Organisations (RTOs).

This Policy is written to comply with:

- The Privacy Act 1988 (Cth) and the 13 Australian Privacy Principles (APPs) the national rules for handling personal information
- The Notifiable Data Breach (NDB) Scheme
- The Standards for Registered Training Organisations (RTOs) 2025, which commenced on 1 July 2025, including the Outcome Standards, the Compliance Standards, and the Credential Policy
- Relevant Commonwealth reporting obligations to bodies such as ASQA and NCVER
- Asuria may update this Policy at any time; the current version will always be published on our website.

2. Scope

This Policy applies to all individuals whose personal information we collect, including:

- Learners, trainees and participants in our training programs
- Job seekers and employment services participants
- Employees, officers, contractors and suppliers
- Trainers, assessors and other RTO personnel
- Applicants for employment
- Individuals whose information is provided to us by third parties
- Asuria is fair, transparent and accountable in the way it collects, uses, discloses and stores personal information.

3. How This Policy Supports the Standards for RTOs 2025

Our privacy, information security and record-keeping practices support compliance with:

Outcome Standards

- Transparency of information for learners and prospective learners
- Learner rights and access to information
- Quality and integrity of training and assessment

Compliance Standards

- Secure management of learner records
- Evidence integrity and audit readiness
- Mandatory record retention periods
- Identity and access controls
- Cybersecurity and data breach response

Credential Policy

- Secure storage of trainer and assessor credential records
- Verification of trainer and assessor qualifications and vocational/industry currency

4. What Information We Collect

Depending on your enrolment or role with us, we may collect personal information and where necessary and permitted sensitive information.

Personal Information

- Name, address and contact details (phone, email, date of birth)
- Your Unique Student Identifier (USI)
- Identification documents (for example, ID used to verify your USI)
- Enrolment and training records — course, results, attendance and assessment outcomes
- Employment history and qualifications
- Driver's licence details, where relevant
- Bank account and payment details, where relevant to fees

- Photographs or video recordings
- Support needs LLN assessment results, disability or access needs, welfare referrals (only what's needed to support you)

Sensitive Information

- We only collect sensitive information with consent, or where permitted or required by law, including:
- Health or disability information
- Criminal history (for example, for employment or work-placement requirements)
- Racial or ethnic origin
- Sexual orientation
- Trade union or professional association membership
- We only collect what we actually need to enrol you, train and assess you, issue your certification, support you, and meet our legal and regulatory reporting obligations.

5. How We Collect Information

We collect information through:

- Enrolment processes
- Training and assessment activities
- Employment services interactions
- Online forms, websites and digital platforms
- Government departments and authorised third parties
- Security sign-in systems
- Complaints and feedback channels
- Where practicable, we collect information directly from you. If we receive unsolicited information that we are not permitted to retain, we will destroy or de-identify it.

6. Why We Collect and Use It

We use your personal information to:

- Enrol you and check you're suited to your chosen course
- Deliver training and assessment, and issue your certificate or Statement of Attainment
- Verify your USI, which we are legally required to do before issuing certification
- Provide support services (such as LLN support or reasonable adjustment) where needed
- Meet legal reporting obligations to government bodies such as ASQA and NCVER
- Verify the identity and credentials of trainers, assessors and staff
- Carry out quality assurance and audit activities
- Contact you about your enrolment or results, or — with your consent — other courses we offer
- We don't use personal information for anything beyond these purposes without telling you or asking your permission first.

7. Who We Share Information With

We only share personal information when we need to, and generally only with:

- Government regulators and agencies we're required to report to, such as ASQA, NCVET and the USI Registry
- Related entities within the Asuria group
- Delivery partners and service providers directly involved in delivering your training, where necessary and appropriate safeguards are in place
- Auditors and other regulatory bodies
- Technology and data storage providers who support our systems
- An employer or other third party but only your certificate or results, and only with your written permission
- Emergency services or authorities, if required by law or to protect someone's safety
- Asuria does not sell personal information and does not share it with marketers or unrelated third parties.

8. How We Keep Your Information Safe

We take reasonable and practical steps to protect information from loss, misuse, interference or unauthorised access, including:

- Restricting access to records to staff who need it to do their job
- Encrypted storage and transmission of digital information
- Secure passwords, login systems and multi-factor authentication (MFA) for our systems
- Keeping physical records (such as paper files) locked away, with access limited to authorised staff
- Regular backups of digital records, with backup testing, so information isn't lost if something goes wrong
- Patch management, system updates, network monitoring and threat detection
- Secure cloud environments
- Regular staff training in information security
- Making sure any third party or software provider we use to store information also has proper security in place

9. Identity and Access Controls

Asuria maintains strict identity and access controls over personal information and student records, including:

- Role-based access permissions
- Multi-factor authentication (MFA)
- Secure onboarding and offboarding processes
- Regular access reviews
- Logging and monitoring of system access
- Segregation of duties for sensitive information
- Only authorised personnel may access personal information, and only for the purposes for which it was collected.

10. Evidence Integrity and Audit Trails

To protect the integrity of training and assessment evidence, and to remain audit-ready, we use:

- Secure digital systems with audit trails
- Version control for assessment tools
- Tamper-proof storage of learner records
- Controlled access to assessment outcomes
- Regular internal audits
- These measures help ensure evidence of training and assessment remains accurate, complete and unaltered.

11. How Long We Keep Your Information

How long we keep your information depends on what it is. Where the guidance below differs from a specific legislative, contractual or ASQA requirement that applies to a record, the longer or more specific period always takes precedence.

Type of Record	Retention Period
AQF certification documentation, testamurs and Statements of Attainment issued	30 years
Assessment evidence (completed tasks, marking records)	At least 2 years after finish of course unless a specific course requires longer.
General enrolment and contact records	As long as reasonably needed for training, reporting, and legal purposes, then securely destroyed or de-identified.
Skills Tasmania Funded Student Eligibility Evidence. Assessment & Attendance Records	7 Years
Smart and Skilled all records	3 years after finish of course

When we no longer need personal information, and we are not legally required to keep it, we securely destroy or permanently de-identify it.

12. Cookies, Analytics and Digital Tracking

We use cookies and analytics tools (such as Google Analytics) to improve user experience on our website and understand how it is used. Users may disable cookies in their browser settings or opt out of analytics tracking.

13. If Something Goes Wrong the Notifiable Data Breach Scheme

If we become aware that personal information has been lost, accessed without permission, or exposed (a 'data breach'), we will:

- Act quickly to contain the issue and limit any harm
- Assess how serious the breach is and who might be affected
- Take immediate remedial action, following our Data Breach Notification Policy
- Notify affected individuals and, where the breach is an 'eligible data breach' under the law, the Office of the Australian Information Commissioner (OAIC)
- Review what happened and fix the gap that allowed it, so it doesn't happen again
- Staff, students and contractors must report suspected data breaches to us immediately.

14. Your Rights Access and Correction

You have the right to:

- Ask us what personal information we hold about you, and to see it
- Ask us to correct any information that's wrong, incomplete or out of date
- Ask questions about how we use or share your information
- Make a complaint if you think we haven't handled your information properly (see Section 16)
- To request access or correction, contact the Asuria Privacy Officer (details in Section 16). We may require proof of identity before actioning a request. If we refuse a request for access or correction, we will provide written reasons and outline your complaint options.

You can also access your own training results and USI transcript at any time through the USI system, if you have a verified USI.

15. Who's Responsible for What

Role	What They Do
Compliance Manager	Oversees this Policy, handles access and correction requests, and manages any data breach response.
IT	Maintains secure systems, backups, encryption and access controls for digital and physical records.
All Staff	Only access student and staff information when needed for their job, and keep it confidential at all times.
Third Parties & Contractors	Follow the same privacy and security standards when handling our students' and staff information on our behalf.

16. How to Raise a Concern Complaints

If you're worried about how your personal information has been handled, you can raise it with us directly through our Complaints and Appeals process, or in writing to:

Asuria Privacy Officer

The Zenith, Level 17, Tower A, 821 Pacific Highway, Chatswood NSW 2067

E: privacyofficer@asuria.com.au

Complaints are handled confidentially and promptly. If you're not satisfied with our response, you can also contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.