ATM
Australian Training Management

ATM POLICY AND PROCEDURE

Privacy and Data Protection Policy and Procedure

1. Purpose

This policy and procedure ensures the lawful, secure, and transparent handling of personal information by Australian Training Management Pty Ltd (ATM). It outlines ATM's obligations and internal practices for the collection, use, storage, disclosure, and disposal of personal information in accordance with the Privacy Act 1988 and the Australian Privacy Principles (APPs). It also establishes ATM's approach to managing data incidents and maintaining the trust of learners and stakeholders through responsible data governance.

2. Scope

This policy applies to all ATM employees, contractors, trainers, assessors, and any third parties who access or handle personal information on behalf of ATM. It covers personal information in all forms, whether held in physical documents, electronic systems, cloud-based platforms, or third-party systems, and applies across the full data lifecycle from collection to disposal.

3. Definitions

- **Personal Information**: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in material form or not (e.g. name, contact details, date of birth).
- **Sensitive Information**: A subset of personal information afforded additional protections under the Privacy Act 1988. In ATM's context this includes information about disability status and learning support needs collected for the purpose of facilitating reasonable adjustments to training delivery, and demographic information collected for AVETMISS reporting (such as Indigenous status or country of birth).
- **Data Breach**: An incident where personal information is accessed, disclosed, lost, or altered without authorisation, in a manner that may cause harm to the individual concerned.
- **AVETMISS**: Australian Vocational Education and Training Management Information Statistical Standard. The national data standard for collection and reporting of VET activity.

4. Policy Statement

ATM is committed to handling personal information lawfully, fairly, and transparently. ATM collects only the information necessary for the delivery of training and assessment services, protects that information from unauthorised access or misuse, and ensures individuals can access and correct their own information. All staff are required to handle personal information in accordance with this policy and the Australian Privacy Principles.

5. Roles and Responsibilities

General Manager:

- Policy owner. Reviews and approves this policy annually or as required.
- Final escalation point for serious data breaches, regulatory notifications, and unresolved privacy complaints.
- Determines whether regulatory notification to the Office of the Australian Information Commissioner (OAIC) is required.

Business and Finance Manager:

- Second escalation point for privacy matters referred by the Compliance Team, including potential data breaches, unresolved access or correction requests, and complaints involving sensitive information.
- Coordinates ATM's response to data breach incidents and escalates to the General Manager where required.
- Maintains the Data Breach Register and ensures this policy is kept current.

Compliance Team:

- First point of contact for privacy enquiries, access and correction requests, complaints, and reports of suspected data breaches.
- Logs all privacy matters and handles straightforward enquiries and requests at first instance.
- Escalates to the Business and Finance Manager where the matter involves a potential data breach, sensitive information, or cannot be resolved at first instance.

All Staff:

- Handle personal information only as required for their role and in accordance with this policy.
- Report any suspected data breach or privacy incident to the Compliance Team immediately.

IT Administrator (or delegate):

- Ensures secure configuration, access controls, patching, and monitoring of digital systems where personal information is stored.

6. Procedure

6.1 Collection of Personal Information

ATM collects only the personal information that is necessary for the effective delivery of training and assessment services. Information is collected with the individual's knowledge and, where required, their consent, in compliance with the Privacy Act 1988.

Types of information collected

- **Personal details**: Name, date of birth, contact details, and emergency contact information.
- **Demographic information**: Gender, country of birth, language spoken at home, and Indigenous status, collected for AVETMISS reporting or government funding purposes.
- **Education and training details**: Prior qualifications, assessment records, and training outcomes.
- **Employment information**: Employer details, job role, and supervisor information for traineeship or apprenticeship enrolments.
- **Learning support needs**: Disability status and learning support needs, collected for the sole purpose of facilitating reasonable adjustments to training delivery in accordance with the Disability Discrimination Act 1992.
- **Financial information**: Payment details for course fees and eligibility information for government subsidies or funding.

Additional information may be collected where required under AVETMISS, State or Territory funding obligations, or regulatory compliance (e.g. ASQA audits).

Collection methods

- Online or paper enrolment and application forms.
- Verbal communications in person or by telephone.
- Training and assessment records.
- Online platforms and digital participation records.

Where consent is obtained via online enrolment forms or portals, it is treated as valid under electronic transactions legislation. Individuals are informed of how their data will be used and are required to acknowledge ATM's privacy policy prior to submission.

6.2 Use and Disclosure of Personal Information

ATM uses and discloses personal information only for purposes directly related to training and assessment services, including:

- Enrolling students in training programs.
- Reporting to ASQA, the Department of Employment and Skills Development, and other government authorities as required by law.
- Confirming student eligibility for government funding and subsidy programs.
- Providing learning support and reasonable adjustments.
- Complying with legal, regulatory, and statutory reporting requirements.

Personal information may be disclosed to:

- ASQA as part of audit and regulatory compliance activities.
- State and Commonwealth government departments, including the Department of Education.
- Employers where the student is a trainee, apprentice, or employer-sponsored learner.
- Contracted trainers, assessors, and service providers under confidentiality arrangements.

Where training or assessment is delivered through third-party arrangements, ATM ensures that data protection obligations are embedded in all relevant agreements. Third parties must comply with the Privacy Act 1988 and maintain secure handling of any personal information accessed on behalf of ATM.

6.3 Storage and Security

ATM takes all reasonable steps to protect personal information from unauthorised access, loss, misuse, disclosure, or modification.

Storage methods

- **Electronic records**: Stored on secure servers with password-protected access and encryption.
- **Hard copy records**: Stored in lockable filing cabinets in secure areas with restricted access.
- **Cloud-based storage**: Information may be stored in secure cloud-based platforms, some of which may be hosted overseas. Where this occurs, ATM ensures that providers maintain privacy protections equivalent to Australian standards, as required under APP 8 (cross-border disclosure of personal information).

Security controls

- Role-based access controls limiting access to student records to staff with a legitimate need.
- Secure login credentials for all electronic systems.
- Firewalls, antivirus software, and encryption for digital records.
- Regular data backups and secure disposal of records when no longer required.

6.4 Access and Correction

Students, staff, and stakeholders have the right to access personal information ATM holds about them, and to request correction of any inaccurate or incomplete information. Requests must be made in writing to the Compliance Team at compliance@australiantraining.com.au.

- **Access requests**: Processed within 10 business days. Proof of identity is required.
- **Correction requests**: ATM will update inaccurate information as soon as practicable to ensure accuracy and completeness.

6.5 Data Retention and Disposal

ATM retains personal information for as long as required by the Standards for RTOs 2025, ASQA, and government funding obligations. Detailed retention periods are set out in the Records Management Policy (ATM-RTO-18).

Key retention periods

- AVETMISS-compliant training activity records may be retained for up to 30 years where required by government contracts.
- Assessment evidence and competency records must be retained for a minimum of 6 months following completion, or longer if required by funding or auditing bodies.

When personal information is no longer required, hard copy records are shredded and digital records are permanently deleted or securely erased.

6.6 Data Breach Response

ATM maintains a procedure for identifying, containing, and responding to data breaches. As a private RTO with a turnover under $3 million that does not hold health information, ATM is not currently a prescribed entity under the Notifiable Data Breaches Scheme (NDBS). However, ATM voluntarily follows the NDBS notification steps as best practice to protect individuals and maintain trust.

Breach response steps

- **Identify**: Staff report the suspected breach to the Compliance Team immediately. The Compliance Team confirms whether a breach has occurred, logs it in the Data Breach Register, and escalates to the Business and Finance Manager.
- **Contain**: The Compliance Team takes immediate steps to limit further exposure or loss of information.
- **Assess**: The Business and Finance Manager assesses the type, scope, and potential harm of the breach and escalates to the General Manager where the breach is serious or may require regulatory notification.
- **Notify**: Where individuals may be at risk of harm, the General Manager determines whether affected individuals should be notified and whether the Office of the Australian Information Commissioner (OAIC) should be informed.
- **Review**: Conduct a post-incident review to identify control gaps and implement corrective actions. Record as a corrective action in the Continuous Improvement Register.

7. Complaints and Concerns

Any person who believes their personal information has been mishandled by ATM may lodge a written complaint with the Compliance Team at compliance@australiantraining.com.au. The Compliance Team will acknowledge the complaint within 5 business days. Where the complaint cannot be resolved at that level, it will be escalated to the Business and Finance Manager. Where it remains unresolved, the Business and Finance Manager will escalate to the General Manager for final determination. ATM aims to resolve all complaints within 30 business days. If a complainant remains unsatisfied following ATM's internal process, they may contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

8. Compliance References

- Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)
- Standards for RTOs 2025 (ASQA) – Outcome Standards 4.1 and 4.4
- National Vocational Education and Training Regulator Act 2011
- Disability Discrimination Act 1992 (Cth)
- OAIC Guidelines and Notifiable Data Breaches Scheme (voluntary compliance)
- ISO 9001:2015 – Clauses 4.2 (Interested Parties), 6.1 (Risk), and 7.5 (Documented Information)
- ATM-RTO-18 Records Management Policy and Procedure

9. Review

This policy will be reviewed annually or following any change to the Privacy Act 1988, the Australian Privacy Principles, the Standards for RTOs 2025, or ATM's data management practices.

10. Feedback Mechanism

Feedback regarding this policy is welcomed and should be directed to the General Manager at Australian Training Management for review and continuous improvement consideration.

Approval and Revision History:
Original Issue Date: 06/06/25
Approval Date: 25/08/2026
Approving Authority: Aaron Leafe – General Manager
Effective Date: 25/08/2026

Revision History

Version	Revision Date	Approved Date	Summary of changes	Approved by
V1.0	24/01/2025	24/01/2025	Initial release	Aaron Leafe
V1.2	20/02/2025	21/02/2025	Updated complaints email address	Aaron Leafe
V1.3	27/05/2025	06/06/2025	Updated to reflect Standards for RTOs 2025 and clarified breach conditions	Aaron Leafe
V1.4	07/07/2026	25/08/2026	Format alignment to ATM standard. Header corrected to ATM POLICY AND PROCEDURE. Privacy Officer title removed; no individual formally designated. Policy ownership assigned to General Manager. Three-tier escalation path established: Compliance Team (first contact) – Business and Finance Manager (second escalation) – General Manager (final escalation). Breach response procedure updated to reflect escalation path. Complaints section updated to reflect escalation path and removed direct BFM contact. Access and correction requests directed to Compliance Team. Sensitive information definition narrowed. NDB Scheme reframed as voluntary compliance. Compliance references updated. DDA 1992 added.	Aaron Leafe