1. Purpose

AAMC Training Group Pty Ltd ("AAMC Training Group") is committed to protecting the privacy and confidentiality of our students, staff, contractors, and stakeholders.

We operate in accordance with:

- Standards for RTOs 2025
- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Data Provision Requirements 2012
- Student Identifiers Act 2014.

The purpose of this policy is to outline:

- The type of personal information we collect and hold
- How we collect, store, use, and disclose personal information
- How individuals can access or correct their personal information
- How we protect and manage personal information
- The processes for raising privacy concerns or complaints.

2. Policy Statement

AAMC Training Group will:

- Collect only the personal information required for legitimate business, training, and assessment purposes or as required by law
- Use personal information only for the purposes for which it was collected, unless permitted by law or with consent
- Securely store all personal information to protect against misuse, loss, and unauthorised access
- Provide individuals with access to their personal information and the opportunity to request corrections
- Provide a copy of this Privacy Policy upon request and ensure it is published on our website.

3. Definitions

a) **Personal Information** – Information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and recorded in any form.

b) **Sensitive Information** – A subset of personal information that includes details about racial/ethnic origin, political opinions, religious beliefs, professional memberships, sexual orientation, or criminal record.

4. Open and Transparent Management of Personal Information

4.1 AAMC Training Group will:

a) Manage personal information in a way that is open, transparent, and compliant with the APPs.

b) Provide clear information about what we collect, why we collect it, and how it will be used or disclosed.

c) Respond promptly to enquiries or complaints regarding privacy.

d) State whether personal information may be disclosed overseas (AAMC does not routinely disclose overseas unless specifically authorised by the individual).

4.2 Overseas Hosting and Service Providers

Some third-party systems we use (e.g., learning/student management systems, email or analytics) **may store or process data outside Australia**. Where this occurs, we take reasonable steps to ensure recipients comply with the **APPs**, including contractual privacy and security obligations, encryption in transit and at rest where supported, and vendor due diligence. We will not disclose personal information overseas **unless** required or permitted by law or with your consent.

5. Collection of Personal Information

5.1 Why we collect

We only collect personal information necessary for:

a) Enrolment and participation in training and assessment

b) Reporting to government agencies as required under the National VET Data Policy*

c) Compliance with relevant legislation.

5.2 What we collect

Types of information collected may include:

- Name, date of birth, gender, contact details
- Cultural background, language spoken at home, and country of birth
- Employment and education history relevant to enrolment
- Unique Student Identifier (USI)

  We will verify your USI with the Student Identifiers Registrar. If you have a permitted exemption, we will advise that your results will **not** appear on your authenticated VET transcript and may not be accessible through Commonwealth systems.
- Photo identification (such as a driver's licence)

  We may collect and store copies for the purposes of verifying your identity for enrolment, skills role plays, online assessments, video assessments, RPL applications, or any other assessment-related authenticity requirements. We may also collect video recordings or photographs submitted as part of assessment evidence. This information is used solely to

confirm student identity, ensure the integrity of our assessment processes, and meet regulatory and audit obligations.

All identification documents and images are stored securely and accessed only by authorised staff in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles.

- Any other information required by government data collection frameworks.

5.3 How we collect

Collection methods include:

Enrolment application forms (online)

- Direct contact (phone, email, in-person)
- Third-party confirmations (e.g., previous training providers, licensing authorities – with consent).

We will notify individuals when collecting information from a third party, except where this poses a serious health/safety risk.

Where a learner is **under 18**, we may require **parent/guardian consent** for collection, use and disclosure of personal information, consistent with the APPs and applicable state/territory laws.

5.4 NCVER and National VET Data Policy

AAMC Training Group is required under the **National VET Data Policy** to collect, hold, use and disclose student personal information to the **National Centre for Vocational Education Research (NCVER)**. Your information may be used for:

- administering VET, including program administration and regulation;
- facilitation of statistics and research relating to education;
- understanding and improving VET, including surveys; and
- administration, including determination of eligibility for funding.

NCVER may disclose your information to the Australian, state and territory governments and agencies, and researchers. You may be contacted to participate in a survey by NCVER, a government department, agent, or contractor. For more information, see the NCVER Privacy Policy.

5.5 Website Cookies

Our website uses cookies to:

- Maintain user sessions
- Analyse usage patterns (Google Analytics, Alexa)
- Provide tailored content and marketing where consented.

Users can manage or block cookies through their browser settings. Cookie data retention varies by type (from per-session to 1.5 years).

6. Use and Disclosure of Personal Information

We will only use or disclose personal information for:

- The purpose for which it was collected
- A related secondary purpose the individual would reasonably expect
- Situations authorised by law (e.g., reporting to NCVER, ASQA, funding bodies)
- Circumstances involving health or safety risks, or law enforcement activities.

We will not sell or rent personal information to third parties.

6.1 Direct Marketing

a) We may send information about AAMC services and benefits where the individual has provided consent

b) An easy "opt-out" option is provided in all communications

c) We comply with the **Spam Act 2003**. Every marketing message includes a functional **unsubscribe**. Opt-out requests are actioned promptly.

6.2 Cross-Border Disclosure

We will not disclose personal information to overseas recipients without the individual's prior written consent, unless required by law.

6.3 Government Related Identifiers

We are required by law to collect and report the USI but will not adopt it as our own identifier and will not display it on certificates.

6.4 Third-Party Service Providers

We engage trusted service providers (e.g., LMS/SMS, payment gateways, IT support, analytics) who may access personal information **only to the extent necessary** to provide their services. All such providers are bound by confidentiality and privacy obligations and must implement appropriate security controls.

7. Integrity & Security of Personal Information

We will take reasonable steps to:

- Ensure personal information is accurate, up to date, and complete
- Protect against misuse, loss, unauthorised access, or disclosure
- Destroy or permanently de-identify personal information when no longer required by law.

7.1 Security controls

We apply proportionate technical and organisational measures, including role-based access controls, multi-factor authentication, encryption in transit (TLS) and at rest where supported, regular backups, least-privilege access, secure disposal/destruction, staff privacy training, and vendor risk management.

8. Access & Correction

Individuals may access their personal information via the Learning Management System (LMS) for real-time student records or via email to info@aamctraining.edu.au.

- Requests will be responded to within 30 days or sooner.
- Correct inaccurate information upon request, unless there are lawful reasons not to.
- AAMC Training will provide written reasons if access or correction is refused.

8.1 Responsibilities

- **Management** – Ensures compliance with the Privacy Act 1988, APPs, and this policy; monitors privacy practices and continuous improvement
- **Staff** – Handle personal information in accordance with this policy and legislative requirements
- **Students** – Keep personal details up to date.

8.2 Records Management

Personal information is managed in accordance with our **RTO Reporting and Records Management Policy**.

8.3 Retention & Disposal

We retain and dispose of records in line with VET and legal requirements, including:

- **Assessment evidence**: minimum **2 years** (or longer if required by funding contracts or federal traineeship regulations);
  a) **Funded training records (where applicable)**: up to **7 years** (state/territory rules apply);
  b) **Credential issuance records**: **30 years**;
  c) **Complaints/appeals records**: minimum **5 years**;
  d) **General student files**: as per **Records Management Policy** and applicable laws.

Records are securely destroyed or permanently de-identified when retention periods expire.

8.4 Monitoring & Review

This policy will be reviewed annually or sooner if legislative or ASQA requirements change.

Feedback and complaints will be handled under our **Complaints Policy & Procedure** and **Appeals Policy & Procedure**.

9. Data Breach Response

AAMC Training Group manages suspected or actual data breaches in line with the **Privacy Act 1988** (NDB scheme). We will:

a) promptly contain and assess any suspected breach;

b) within **30 days**, determine if the breach is likely to result in **serious harm**;

c) if notifiable, prepare a statement to the **Office of the Australian Information Commissioner (OAIC)** and **notify affected individuals** as required; and

d) record the breach, causes and remediation in our incident register and Continuous Improvement process.

This is detailed in our **Data Breach Policy.**

9.1 Privacy Complaints – External Escalation

If you are not satisfied with our response, you may contact the **Office of the Australian Information Commissioner (OAIC)**: www.oaic.gov.au / 1300 363 992.