PRIVACY POLICY AND PROCEDURE

1. SCOPE

Tactical Training (Australia) Pty Ltd (TTA) is committed to maintaining the privacy and confidentiality of its RTO personnel and VET student records. TTA complies with the *Privacy Act 1988 including the* Australian Privacy Principles (APPs) and with the ***National Vocational Education and Training Regulator (Outcome Standards for NVR Registered Training Organisations) Instrument 2025 (Standards)*** *and* ***(Compliance Standards for NVR Registered Training Organisations*** *and* ***Fit and Proper Person Requirements) [Compliance Standards]****.*

2. AUDIENCE AND APPLICABILITY

The *Privacy Policy and Procedure* applies to all TTA staff involved in accessing and handling private, confidential and sensitive information, in particular information that may identify an individual, including:

- Names
- Addresses
- Phone numbers
- Emails
- Photos
- Bank account details
- Medical records

3. PURPOSE

This policy sets out the commitment of TTA to ensure responsible and safe handling of private, confidential and sensitive information.

TTA is a small business with an annual turnover of $3,000,000 and is currently exempt from mandatory compliance with the Australian Privacy Principles (APPs). However, TTA may, in future, engage as a contractor for the Commonwealth Government or enter into agreements with government agencies that require adherence to the APPs. In anticipation of such obligations and to uphold best practice standards, TTA has proactively chosen to comply with the APPs.

TTA manages personal information in an open and transparent way. This is evident in the implementation of practices, procedures, and systems we outline in this policy, that ensure our compliance with the APPs and any binding registered APP codes. These practices provide suitable procedures for TTA personnel to deal with related inquiries.

Requirements under the Compliance Standards

Requirements for handling private information in relation to the ***Compliance Standards***:

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.

National VET Data Policy

While TTA, as an RTO, does not fall under the definition of an 'APP entity' under the *Privacy Act 1988*, responsibilities exist under the ***National VET Data Policy***:

4. Data provision requirements

4.4 All RTOs must:

(d) When collecting data for the National VET Provider Collection form students, comply with APP 3 and 5 of the Privacy Act 1988 as if it were an APP entity under that Act

7. Mandatory notifications to data providers

7.1 It is the responsibility of RTOs to ensure students who provide an RTO with personal information that will be included in the National VET Provider Collection are reasonably aware the information may be collected, used or disclosed for the purposes set out in the Privacy Notice at Schedule 1 of the Policy.

7.2 Where personal information is collected from a student, RTOs must make students aware of the purposes for which their information may be collected, used or disclosed. RTOs must give the student a copy of the Privacy Notice at Schedule 1 of this Policy. This can be achieved by including the 'Privacy Notice' during the student's enrolment process. The minimum mandatory content for inclusion in a Privacy Notice is at Schedule 1 of this Policy.

7.3 Version 2 of the Policy commenced on 1 January 2019, however RTOs had until 1 July 2019 to transition to the new Privacy Notice at Schedule 1.

7.6 Additional requirements may apply to RTOs. Section 7 of this Policy is confined to VET Data collected, used or disclosed under the National VET Data Policy and is not meant to address all of the possible ranges of obligations or responsibilities to which an RTO may be subject, including privacy obligations.

Australian Privacy Principles

The following information is sourced from the *Australian Privacy Principles quick reference* (https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference)

APP1 Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP2 Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP3 Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.

APP4 Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP5 Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.

APP6 Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP7 Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP8 Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP9 Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP10 Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP11 Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP12 Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP13 Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

The *Privacy Act 1988* may be viewed at:
https://www.legislation.gov.au/

The Australian Privacy Principles guidelines may be viewed in full at:
https://www.oaic.gov.au/privacy/australian-privacy-principles

As an NVR Registered Training Organisation, regulated by Australian Skills Quality Authority (ASQA), TTA is required to collect, hold, use, and disclose a wide range of personal and sensitive information of VET students participating in nationally recognised training products. This information requirement is outlined in the *National Vocational Education and Training Regulator Act 2011* and associated legislative instruments. In particular, the legislative instruments:

- *National Vocational Education and Training Regulator (Outcome Standards for NVR Registered Training Organisations) Instrument 2025*
- *National Vocational Education and Training Regulator (Compliance Standards for NVR Registered Training Organisations and Fit and Proper Person Requirements) Instrument 2025*
- *Student Identifiers Act 2014*
- *National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020*
- *National VET Data Policy*

It is further noted that, aligned with these requirements, TTA may at times deliver services through a range of Commonwealth and State Government funding agreements, that will include various information collection and disclosure requirements, and may therefore be subject to Privacy laws.

4. DEFINITIONS

The Definitions within the *Standards* defines certain words and expressions which have specific meaning in the *Standards*. TTA and all staff will defer to the definitions as published in the *Standards* where relevant.

Words and expressions that remain undefined in the *Standards* take on dictionary meaning under the direction of the ASQA.

For this policy document, TTA has identified the necessity to define the following expressions:

AQF certification documentation means the set of official documents which confirm that an AQF qualification or VET statement of attainment has been issued to an individual by an NVR registered training organisation or any other entity authorised to do so. *[Definitions within the Standards]*

Australian Privacy Principles (APP) are guidelines that outline the mandatory requirements of the APP, how they interpret the APP's, and matters they may take into account when exercising functions and powers under the *Privacy Act 1988.*

Australian Skills Quality Authority [ASQA] means the National VET Regulator for Australia's vocational education and training sector. As referenced within the *National Vocational Education and Training Regulator Act 2011 (S155(2))*.

Complaint means a statement that something is unsatisfactory or unacceptable. *[Oxford Languages]*

Complaints arise when a person is not satisfied and requests action to be taken to resolve the matter. These matters can include unfair or unjust treatment in the assessment process, unjust disciplinary measures, sexual harassment, or any failure to adhere to the principles of equality of opportunity in education or employment. It does not matter whether a person suffers an injustice or only thinks so. Goodwill is damaged either way unless there is a chance to air the complaint and seek mutually acceptable resolution and outcomes. *[TTA]*

Compliance Standards means the *National Vocational Education and Training Regulator (Compliance Standards for NVR Registered Training Organisations and Fit and Proper Person Requirements) Instrument 2025.*

Destroying or de-identifying personal information means reasonable steps that are taken to destroy or de-identify personal information held by the RTO once it is no longer needed for any purpose for which it may be used or disclosed under the APP.

Notifiable Data Breach refers to the loss of personal information an organisation or agency holds or where information is subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person.

(Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/)

Office of the Australian Information Commissioner [OAIC] refers to the independent national regulator for privacy and freedom of information.

Personal information is defined as "a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances" and may include but is not limited to an individual's name, signature, address, telephone number, date of birth, sensitive information, credit information, employee records information, photographs.

(Source: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information)

Privacy Notice describes how an entity handles personal information collected from the student that may be used together with training activity information. The Privacy Notice lists the ways information about the student is collected and why, and how it is used and shared. The minimum mandatory content for inclusion in a Privacy Notice can be found at Schedule 1 of this Policy. [Ref: *National VET Data Policy*].

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

(Source: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information)

Student Identifier has the same meaning as in the *Student Identifiers Act 2014*. *[Definitions within the Standards]*

5. POLICY AND PROCEDURES

TTA has conducted an analysis of the risks associated with the handling of private, confidential, and sensitive information. The following processes and procedures are implemented to mitigate the risks associated with the management of personal information at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction, and de-identification.

5.1 System for management of information

TTA collects, retains, uses, and discloses student data, including personal data. The information is collected for the sole purpose of meeting regulatory, legislative, and contractual requirements relating to training and assessment or the provision of services by TTA in the course of its business operations. TTA is required to collect, hold, use, and disclose information from VET students and other stakeholders for a range of purposes, including but not limited to:

- **Enrolment and Administration**: personal details are requirement to process and manage student enrolments.
- **Regulatory Compliance**: RTOs must comply with laws such as the *National Vocational Education and Training Regulator Act 2011*, which requires reporting of student data to authorities like the *National Centre for Vocational Education Research (NCVER).*
- **Student Identifier:** Personal information ensures that the student's USI number can be verified, located, or created as required to receive qualifications and certifications upon course completion.
- **AQF Certification Documentation**: Personal information ensures that students receive valid qualifications and certifications upon course completion.
- **Funding and Government Reporting**: Where training programs receive government funding, RTOs must provide student data to agencies for funding eligibility and reporting.

VET students and other stakeholders are advised that due to these legal requirements, TTA is required to disclose personal information for valid purposes to entities including:

- Governments (Commonwealth, State, or Local)
- Australian Skills Quality Authority (ASQA)

- National Centre for Vocational Education Research (NCVER)
- Student Identifiers Register, under the *Student Identifiers Act 2014* (Commonwealth)
- Employers (and their representatives), employment services, or return to work providers, schools, guardians, or other authorised persons.

5.2 What information is collected

TTA collects various types of personal information to manage student enrolments, track progress, and report data to the National Centre for Vocational Education Research (NCVER).

We may collect personal information, including but not limited to:

- **Contact Details**: Name, address, email address, phone number.
- **Identification**: e.g. Driver's licence, Medicare Card, Passport, VISA, Birth Certificate
- **Personal Identifiers**: Date of birth, Student IDs, USIs.
- **Demographics**: Age, gender, language spoken at home, Indigenous status, disability status, employment information.
- **Training and assessment information**: Enrolment details, training outcomes, assessment results.

5.3 Personal identification documentation

As an RTO, TTA requires students to present identification documents to verify a student's eligibility for training programs. This is necessary for several reasons:

- **Confirming Citizenship or Residency**: TTA must ensure that students meet citizenship or residency requirements for participation in nationally recognised training.
- **Creating a USI:** TTA must gather the necessary identification documents to generate and verify Student Identifiers.
- **Regulatory Compliance**: RTOs must comply with the Standards and other directions as given by the ASQA and other government regulations.
- **Fraud Prevention**: Verifying student identities safeguards the integrity of enrolments, preventing fraudulent participation and ensuring authenticity.

5.4 How information is collected

Personal information is collected through a variety of methods to manage student enrolments and to comply with regulatory requirements. Information is collected in the following ways:

- **Enrolment Forms**: Students provide personal details such as name, date of birth, contact information, and identification documents during the enrolment process.
- **Online Portals:** Students may submit their information securely via digital platforms, such as online booking via TTA's website.
- **Surveys and Feedback**: TTA collects additional information through student satisfaction surveys and course evaluations.

5.5 How information is used

RTOs use personal information for various purposes, primarily to manage student enrolments and comply with regulatory requirements. The following are examples of how TTA utilises personal data:

- **Student Identification and Enrolment**: Personal details are used to verify student identity, process enrolments, and issue qualifications
- **Personalise the student experience**: Personal information may be used to customise a student's experience to accommodate individual needs.
- **Unique Student Identifier (USI) System**: Personal information is used to create and /or verify a student's USI, which is required for vocational education and training.
- **Compliance and Reporting:** RTOs must report student data to regulatory bodies like ASQA and the National Centre for Vocational Education Research (NCVER).
- **Training and Assessment Records**: Personal information is used to maintain records of student progress, assessments, and certifications.
- **Communication and Support**: Contact details are used for administrative purposes, student support, and course-related updates.

5.6 Accessing and updating information

Students may request access to their personal information and ask for corrections if any details are inaccurate or outdated in compliance with the Australian Privacy Principles (APPs).

The process for student access and updates to personal information is as follows:

- Students can submit a request to access and/or update their information via the customer care team either in person, over the phone or via email.
- The student's identity will be verified using existing records or additional identification documents.
- If requesting information to be updated, students must specify the information to be changed and provide supporting documents if required.
- Requests to access will be processed within a reasonable timeframe
- Where access is granted, the student will receive a copy of their personal information securely.
- If updates are requested, TTA ensures the changes comply with regulatory requirements.
- The student will be informed about the status of their request and confirmation of changes will be notified.
- All requests for updates and/or changes will be logged within the VETtrak student management system.

5.7 Destructing and De-identifying Personal and Sensitive Information

TTA retains the following in compliance with regulatory, legislative or contractual requirements:

- Records of AQF certification documentation are retained for a period of thirty (30) years within the VETtrak student management system. Access to personal records may be requested in writing by students.
- Physical copies of student files and records of all assessments submitted are retained for a period of 2 years after the student has completed the training product, as per the *Compliance Standards* requirement *10 Records of AQF certification documentation and assessments*. After this time the physical student file will be securely destroyed, and access to the record will no longer be available to the student.

TTA will securely destroy or de-identify all personal and sensitive information, once it is no longer required for any purpose. This forms a key component of their risk mitigation strategy and ensures full compliance with all relevant legislative requirements.

TTA securely destroys or de-identifies personal and sensitive information using the following methods:

- **Onsite shredding of physical documents** to ensure immediate and secure disposal.
- **Engaging a certified confidential document destruction service** for offsite shredding.
- **Digital wiping of electronic data** that is no longer required, using industry-standard deletion protocols.

5.8 Security of information

TTA takes reasonable steps to protect personal information from unauthorised access, misuse, and loss. Data security measures include:

- Ensuring data is collected only when necessary and in compliance with regulatory requirements.
- Storing personal information in encrypted databases (VETtrak student management system) and secure physical locations.
- Restricting and enforcing data access controls to authorised RTO personnel only.
- Conducting internal training of staff on safe handling of personal information and data protection best practices.
- Ensuring staff understand their responsibilities in handling personal information securely.
- Ensuring staff sign the Employee Handbook which requires them to work in accordance with all policies and procedures including *IT Acceptable Use Policy and Procedures and Information Security Policy* and *Procedure*.
- Disabling network account access and recovering all items of property when employees leave TTA.
- Managing and regularly updating firewalls and security software to prevent cyber threats.
- Retaining personal information only for the required period under legal and regulatory guidelines.
- Securely disposing outdated records using shredding, de-identification, or digital wiping.

5.9 Data breach response plan

TTA follows a structured process to respond to data breaches should they occur:

Step 1: Identify and contain

Any staff member or contractor who becomes aware of a potential breach must immediately notify the Compliance Manager or other senior manager.

The Compliance Manager will:

- Assess the situation and take immediate action to contain the breach.
- Implement containment measures, such as revoking access to compromised systems, resetting passwords or shutting down compromised systems.
- Keep detailed records of the incident, including what data was involved, when it occurred, and how it was discovered.

If the breach stems from a third-party provider, the Compliance Manager will:

- Contact the provider to confirm the nature and scope of the breach (via direct contact or existing status line systems).
- Obtain documented confirmation of the incident, including details of affected data and remedial actions taken.
- Ensure contractual obligations regarding data breaches (e.g., notification timelines, cooperation) are enforced.

Step 2: Investigate and risk assess

The Compliance Manager, in consultation with relevant personnel and a professional IT service provider, will assess:

- The nature and extent of the breach.
- The risk of serious harm to affected individuals.
- Whether remedial action has mitigated the risk.

For third-party breaches:

- Evaluate the provider's response, security measures, and any ongoing risks to TTA systems or data.

Step 3: Notify and report

If the breach is a notifiable data breach, TTA will:

- Notify affected individuals, providing the following information:
    - The RTO's name and contact details.
    - A description of the data breach.
    - The type of personal information involved.
    - Recommended steps individuals should take to mitigate the risk.
- Direct notification via email or letter is the preferred method of communication. Where this cannot be achieved or is not practicable, indirect notification may be used via public notice on the TTA website.
- Contact the Office of the Australian Information Commissioner (OAIC) for advice on reporting obligations. (TTA has no obligations under the Privacy Act – organisations that are subject to the Act must use the Notifiable Data Breach Form to notify OAIC): (https://webform.oaic.gov.au/prod?entitytype=DBN&layoutcode=DataBreachWF).

If the breach involves a third-party provider:

- Include the provider's name and a summary of their role in the incident in notifications, where appropriate.

Step 4: Review and improve

TTA will conduct a post-incident review to:

- Identify the root cause of the breach and document lessons learned.
- Implement corrective actions:
    - Update policies and procedures based on findings, revise the data breach response plan, privacy policy, and other relevant policies.
    - Implement security enhancements to address any identified vulnerabilities, such as implementing stronger access controls, better encryption, and enhanced firewalls.
    - Provide staff training to ensure all staff understand privacy obligations, data security practices, and updated policies and procedures.

For third-party breaches:

- Review the provider's compliance with contractual and legal obligations and consider whether to continue the relationship or impose additional security requirements.

5.10 Privacy complaints procedure

TTA will address all complaints received in relation to privacy information in a timely and effective manner.

Students can direct enquiries about the complaints process to the Customer Care team at 08 8331 1620 or via email to customercare@tacticaltraining.edu.au. The Customer Care team will advise them how to submit a complaint.

Lodging a Privacy complaint with TTA

Students will be requested to provide details in writing by submitting a letter or via email using the following contact methods:

Address: The Privacy Officer
Tactical Training (Australia) Pty Ltd
3/190 Glynburn Road, Tranmere SA 5073

Email: privacy@tacticaltraining.edu.au

TTA will investigate the circumstances included in the complaint and will respond to the individual as soon as possible (within 30 calendar days) regarding its findings and the proposed actions following the investigation.

Lodging a Privacy complaint with Office of the Australian Information Commissioner (OAIC)

Where the student is not satisfied with the decision of the RTO they will be referred to the national regulator, the Office of the Australian Information Commissioner (OAIC) where complaints can be submitted in the following ways:

By completing an online form here:

https://webform.oaic.gov.au/prod?entitytype=Complaint&layoutcode=ComplaintWF

By downloading and completing a Privacy Complaint Form that is accessible from:

https://www.oaic.gov.au/__data/assets/word_doc/0010/1135/privacy-complaint-form-v4.docx

Complaint forms can be sent by mail to:

Office of the Australian Information Commissioner, GPO Box 5288, Sydney NSW 2001

Enquiries for the OAIC can be directed to:

Phone: 1300 363 992

Website: https://www.oaic.gov.au/

When investigating a complaint, the OAIC will initially attempt to conciliate the complaint, before considering the exercise of other complaint resolution powers.

Lodging complaints about an RTO with Australian Skills Quality Authority (ASQA):

Alternatively, if the complaint relates to a non-privacy matter, or should individuals choose to do so, a complaint may also be lodged with the ASQA complaints handing service for complaints against RTOs:

Website: https://asqaportal.asqa.gov.au/Make-a-Report/

Telephone: 1300 701 801

6. POLICY PROMOTION

Access to this Policy is accessible via the following means:

- To staff members, via the Public Drive on the Server.
- Terms of this policy are promoted in information provided and throughout student's pre-enrolment and enrolment process.
- To students in hard copy format, upon request to the TTA Customer Care team.
- Available to students and other clients of TTA through publication in Terms & Conditions on www.tacticaltraining.edu.au/information/terms-and-conditions

Policy documents that are accessed as described above are original Controlled Documents. All other printed, copied and photocopied versions of these documents are Uncontrolled Documents and are subject to change at any time. Readers must check the version control of the document prior to official use.

7. REVIEW OF POLICY

TTA will review the *Privacy Policy and Procedure* every 12 months or on an as needs basis (whichever occurs first).

8. ENDORSEMENT

Prepared by: Compliance Manager

Approved by: Chief Executive Officer

Date of effect: 23rd October 2025

Next review date: October 2026