Privacy Policy & Procedure

Purpose:
This policy documents Technical Advanced Training, proactive commitment to ensuring the privacy of all documentation and personal information in all forms, forums and media. In this commitment, Technical Advanced Training will follow the ten national privacy principles in the handling of personal information of trainees / employees.

Scope:
This policy covers all training function activities and documents associated with the AQTF Standards for Registered Training Organisations. It is also a core part of *Legislation Information for Students and Trainers* and *Training Records Policy and Procedures* which covers individual components of privacy compliance that Technical Advanced Training adheres to under AQTF requirements.

Definitions:
Training Records covers all documentation and information relating to training and assessment activities. It includes but is not limited to:

- student enrolment data;
- commencement and completion dates for individuals of all competency units;
- individual student assessment information for each unit of competency;
- information on awards issued (award, date, certificate number);
- individual student participation data (assignments / assessments where practicable, attendance)
- documentation / records of grievances, complaints, appeals
- recognition (RPL/RCC) process documents (application and results)

Policy:
1. Technical Advanced Training is committed to maintain and safeguard the confidentiality and privacy of all individual student information. It will document and implement procedures to assure the integrity, accuracy and currency of records.
2. Individual student records will be stored (including the backup of all electronic records) in a secure area and with safeguards in place to minimise loss, unauthorised access and use, modification or misuse.
3. Student results will be archived for a period of not less than 30 years.
4. Training records will be collected and stored to meet the requirements of external reporting requirements.
5. Access to individual student training records must meet Commonwealth and State Privacy legislation and will be limited to:
    - Individuals wishing to access their personal records
    - Individuals authorising releases of specific information to third parties
    - Technical Advanced Training staff that require the information for their job role
    - Office of Training and Tertiary Education or their representative for activities under the Standards for Registered Training Organisations
    - Legal requirements (eg. subpoena / search warrants / social service benefits / evidence act)
6. Technical Advanced Training' Training Manager will be the person responsible for the implementation and maintenance of the policy.

Procedure:

1. Each individual student will have a personal file for storage of training records.
2. Student training documentation will be stored in a secure manner (individual files in locked cabinets; electronic files with access by password).
3. All trainers / assessors involved in the program will be informed of their responsibilities under this policy.
4. Requests for access to the information must be in writing and the release of information the decision of Technical Advanced Training' Training Manager.
5. Records of student results for each unit of competency will be as per VRQA requirements so as to limit the amount of rework.
   The 2010 VRQA requirements for student results for each unit of competency are:

Value	Description
20	Competency achieved / pass
30	Competency not achieved / fail
40	Withdrawn
50	Recognition of Prior Learning
60	Credit Transfer
70	Continuing enrolment
81	Non-assessable enrolment – Satisfactorily completed
82	Non-assessable enrolment – Withdrawn or not satisfactorily completed
90	Result not available

Information on Technical Advanced Training' Training Records Policy and Procedures will be included in student and trainer / assessor folders.

6. Information to be retained as a minimum, but not limited to:
   a. Student full name,
   b. Date of Birth,
   c. Address,
   d. Enrolment / commencement date,
   e. Course code
   f. Course Title,
   g. Unit of Competency / Module code,
   h. Unit of Competency / Module title,
   i. Result
   j. Credit transfer,
   k. Date finished.

Ten National Privacy Principles

1. Collection - The organisation will collect only the information necessary for one or more of its functions. The individual will be told the purposes for which the information is collected.
2. Use and disclosure - Personal information will not be used or disclosed for a secondary purpose unless the individual has consented or a prescribed exception applies.
3. Data quality - The organisation will take all reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.
4. Data Security - The organisation will take all reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
5. Openness - The organisation will document how they manage personal information and when asked by an individual, will explain the information it holds, for what purpose and how it collects, holds, uses and discloses the information.
6. Access and correction - The individual will be given access to the information held except to the extent that prescribed exceptions apply. The organisation will correct and up date information errors described by the individual.
7. Unique Identifiers - Commonwealth Government identifiers (Medicare number or tax file number) will only be used for the purposes for which they were issued. The organisation will not assign unique identifiers except where it is necessary to carry out its functions efficiently.
8. Anonymity - Wherever possible, the organisations will provide the opportunity for the individual to interact with them without identifying themselves.
9. Transborder Data Flows - The individual's privacy protections apply to the transfer of personal information out of Australia.
10. Sensitive Information - The organisation will seek the consent of the individual when collecting sensitive information about the individual such as health information, or information about the individual's racial or ethnic background, or criminal record.