Privacy Policy

1. Purpose

Australian Institute of Compliance Professionals (AICP) is committed to providing quality training and assessment in accordance with the Standards for Registered Training Organisation 2015 (SRTOs). As such, AICP is required to comply with Federal law regarding Privacy and confidentiality of employees, learners and contractors.

The purpose of this policy is to outline how AICP complies with Privacy Act 1988 and Australian Privacy Principles (APPs).

2. Policy Statement

AICP is committed to complying with obligation under Privacy Act 1988, and the associated Australian Privacy Principles (APPs), specifically in the way it collects, uses, secures and discloses personal information. AICP is committed to safeguarding any confidential information obtained by the RTO.

AICP will ensure :

- It maintains and provides a current Privacy Policy;
- Information gathered for the express purpose of training and assessment matters will not be disclosed to a third party unless prior written consent is provided by the individual concerned, except that required by law;
- The secure storage of all records;
- The confidentiality of all information maintained on records.

3. Policy Principles

3.1 Legislation

a) AICP abides by the Privacy Act 1988.

b) The APPs came into force on 12 March 2014 and set out standards, rights and obligations for the handling, holding, accessing and correction of personal information (including sensitive information).

3.2 Underpinning Principles

a) *Personal Information* is defined in the Privacy Act 1988 to mean "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

   i. whether the information or opinion is true or not; and

   ii. whether the information or opinion is recorded in a material form or not.

b) *Sensitive Personal Information* is defined in the Privacy Act 1988 to mean "information or an opinion about an individual's" that is also personal information, such as:

   i. racial or ethnic origin; or

   ii. political opinions; or

   iii. membership of a political association; or

iv. religious beliefs or affiliations; or
v. philosophical beliefs; or
vi. membership of a professional or trade association; or
vii. membership of a trade union; or
viii. sexual orientation or practices; or
ix. criminal record.

3.3 PART 1 – Consideration of Personal Information Privacy

a) Open and Transparent Management of Personal Information.
AICP will :

i. Ensure that personal information is managed in an open and transparent way.
ii. Take reasonable steps to implement practices and procedures that will facilitate dealing with enquiries or complaints from individuals regarding compliance with the Australian Privacy Principles (APPs).
iii. Ensure that it maintains an up-to-date policy about the management of personal information.
iv. Ensure that AICP Privacy Policy contains the following information:
- The kind of information that is collected and held;
- How the information is collected and held;
- The purposes for which information is collected, held, used and disclosed;
- How an individual may access their personal information that is held by AICP and seek correction of such information as necessary;
- How the individual may make a complaint about a breach of the APPs and how AICP will deal with such a complaint;
- Whether AICP is likely to disclose personal information to overseas recipients, and if so the countries in which such are likely to be located.

v. Provide the Privacy Policy free of charge and in such form as appropriate, and as is reasonable.

b) Anonymity and pseudonymity
AICP will :

i. Respect that individuals may not wish to identify themselves when making enquiries on AICP products and services;
ii. However, require full personal details as required by law and for identification purposes from learners.

3.4 PART 2 – Collection of Personal Information

a) AICP will not collect personal information from you unless that information is necessary for one or more of its functions or activities, or is required by law.
b) AICP advises that it is required by law to collect, hold, use and supply personal information, in accordance with the National VET Provider Collection Data Provision Requirements.
c) AICP will take reasonable steps at or before the time of collection to ensure that you are aware of:

i. Who we are and how to contact us;
ii. How to gain access to your own information;

iii. The purpose for which the information is being collected;

iv. Any organisation to which we would normally disclose information of that kind;

v. Any law that requires the particular information to be collected;

vi. The main consequences for the individual if all or part of the information is not provided.

d) AICP collects information from you in the following ways:

i. When you register your interest online, apply for enrolment, request certain services or products, or otherwise contact or do business with us.

ii. Information may be collected from enrolment forms, certified documents, telephone calls, emails, letters sent by you.

iii. Information may be collected from third parties, such as other training providers, regarding confirmation of training and ongoing professional development that you have attended, as permitted by you.

e) Should AICP collect information about you from a third party we will take reasonable steps to ensure that the individual is or has been made aware of the matters listed above except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

3.5 PART 3 – Dealing with Personal Information

a) AICP will not use or disclose personal or sensitive information for any purpose other than what it was collected for, unless the relevant person has provided written consent to use or disclose that information in circumstances that are different to those for which it was collected.

The circumstances where an exception may occur are:

i. Where the use or disclosure of this information is required or authorised by or under an Australian law or a court/tribunal order;

ii. The individual would reasonably expect AICP to use or disclose the information for the secondary purpose;

iii. A permitted health situation exists in relation to the use or disclosure of the information by AICP;

iv. A permitted general situation exists in relation to the use or disclosure of the information by AICP;

v. AICP reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

b) AICP collects your personal information so as to:

i. Process applications;

ii. Manage your enrolment;

iii. Record and maintain your details;

iv. Administer training programs;

v. Record and maintain details of your ongoing training and assessment;

vi. Provide you with details regarding learner services, benefits, and training opportunities;

vii. Notify you about upcoming events and opportunities;

viii. Gain feedback from you;

ix. Communicate with you;

x. Report to relevant authorities as required by law.

c) Direct Marketing
AICP:

i. May use personal information (specifically your name and relevant address details) and information about your preferences for direct marketing (i.e. the communication channels which you prefer for receiving direct marketing from us and the types of products and services in which you are interested in) so as to let you know about our services and benefits, where we have your consent.

ii. Provides an opt-out and/or unsubscribe method that is easily accessible for individuals to request not to receive direct marketing communications.

d) Cross Border Disclosure
AICP:

i. Does not disclose personal information to overseas recipients unless prior written approval is received by the individual who the personal information relates.

e) Adoption, use or disclosure of Government Related identifiers
AICP:

i. Is required by law (*Student Identifier Act*) to collect, maintain and report to relevant Government agencies the individual's Unique Student Identifier (USI) number in accordance with the National VET Provider Collection Data Provision Requirements.

ii. Will not disclose the Unique Student Identifier (USI) number for any other purpose, including on any Certification documents you receive.

iii. Must not adopt the Unique Student Identifier (USI) number as its own identifier of the individual.

3.6 PART 4 – Integrity of Personal Information

a) Quality of personal information
AICP will take steps, as are reasonable, to ensure that the personal information it:

i. Collects is accurate, up to date and complete;

ii. Uses or discloses, is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

b) Security of personal information
AICP will take steps, as are reasonable in the circumstances to:

i. Protect the information from misuse, interference and loss as well as unauthorised access, modification or disclosure.

ii. Destroy the information or to ensure that the information is de-identified.

3.7 PART 5 – Access to, and correction of, Personal Information

a) AICP provides all learners with electronic access to their own personal records, where the individual can update and maintain their own personal information.

b) In some circumstances, AICP may not permit access to individuals for their personal

information. If this is ever the case, AICP will provide full details for the legal reasons for this decision. These may include that AICP believes:

i. That giving access to the information would pose a serious threat to the life, health or safety of the individual, or to public health or public safety; or

ii. Giving access would have an unreasonable impact on the privacy of other individuals; or

iii. The request for access is frivolous or vexatious; or

iv. The information relates to existing or anticipated legal proceedings between AICP and the individual, and would not be accessible by the process of discovery in those proceedings; or

v. Giving access would reveal the intentions of AICP in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

vi. Giving access would be unlawful; or

vii. Denying access is required or authorised by or under an Australian law or a court/tribunal order; or

viii. Both of the following apply:

- AICP has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to AICP functions or activities has been, is being or may be engaged in;
- Giving access would be likely to prejudice the taking of appropriate action in relation to the maters; or

ix. Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

x. Giving access would reveal evaluative information generated within AICP in connection with a commercially sensitive decision-making process.

c) When dealing with requests for access to personal information, AICP will:

i. Respond to request for access within 30 days of the request, if from an individual, and within a reasonable time, if the request is from an organisation; and

ii. Provide access to the information in the manner requested, if it is reasonable and practicable to do so.

d) AICP does not charge a fee for access to personal information. The exception is re-prints of certification documentation previously supplied.

e) With regard to the correction of personal information held:

i. should AICP be satisfied that information is inaccurate, out of date, incomplete, irrelevant or misleading, AICP will take such steps as reasonable to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

ii. Should AICP refuse to correct information, AICP will give written notice to the individual that sets out:

- The reason for refusal
- The mechanisms available to complain about the refusal; and
- Any other matter prescribed by the regulations.

4. AICP Responsibilities

The CEO ensures that all team members are made aware of this policy and its underpinning legislative requirements, and comply with this policy at all times.

The CEO ensures that all learners have access to and awareness of this policy.

5. Records Management

All personal information and records are maintained in accordance with Records Management Policy.

6. Monitoring and Improvement

All practices for Privacy are monitored by the CEO and areas for improvement identified and acted upon.