Privacy Policy and Procedure

Learning Sphere
RTO Code 91718

Compliance Focus

ASQA Standards: Clauses7.5
National Code: Standard 2, 6, 8

Policy Purpose

The purpose of this policy and procedure is to outline the approach to comply with the Privacy Act 1988 (Commonwealth). This business process describes how we collect, manage, use, disclose, protect, and dispose of personal information in accordance with the Australian Privacy Principles (APPs) outlined in Schedule 1 of the Privacy Amendment Act 2012.

Policy Scope

This policy applies to all students currently and previously enrolled in full or part qualifications. All staff are to adhere to this policy and associated procedure. The General Manager (GM) will provide guidance and advice to all staff on the policy.

Policy Overview

We will practice a high standard of care and concern in regard to maintaining the privacy of others in all aspects of our business operations. As such, we are required to comply with Federal law regarding privacy and confidentiality of employees, students, and contractors and to ensure that we follow the Privacy Act and APPs.

Policy

We are committed to complying with the Privacy Act, and APPs in the way we collect, use, secure, and disclose personal information.
We will ensure:

- That we maintain and provide a current Privacy Policy to all staff, students, and clients
- Information gathered for training and assessment matters will not be disclosed to a third party unless prior written consent is provided by the individual concerned, except as required by law
- The secure storage and confidentiality of all records
- That personal information is managed in an open and transparent way
- Take reasonable steps to implement practices and procedures that will facilitate dealing with enquiries or complaints from individuals regarding compliance with the APPs
- Ensure an up-to-date policy about the management of personal information
- That we respect those individuals that may not wish to identify themselves when making enquiries

Definitions

Under the Privacy Act 1988, personal and sensitive information is defined as:

Personal information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Sensitive information

- Includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record that is also personal information, health information about an individual, genetic information about an individual that is not otherwise health information, biometric information that is to be used for the purposes of automated biometric verification, biometric identification and biometric templates.

Privacy Policy and Procedure

Learning Sphere
RTO Code 91718

1. Commitment

- Implementation and compliance with all applicable privacy legislation including the Privacy and Data Protection Act and Data Provision Requirements
- All information in this policy complies with the 13 APPs as outlined in the Privacy Act
- Collecting, usage, storing and accessing personal information for legitimate reasons only
- Informing individuals, the purpose for which personal information is collected and who is informed
- Personal information is only used for the purpose it was collected
- Provide Privacy Statements that set out the parameters of what personal information is collected
- Take reasonable measures to ensure Privacy information is up to date and complete
- Take reasonable business measures to ensure personal information is secure from unauthorised access and disclosure
- An Individual can access personal record and have a copy of personal information provided the information does not identify any others
- Will not adopt, use, or disclose a government related identifier of an individual

2. Australian Privacy Principles

All staff are to be aware of responsibilities and how they will be applied. The APPs cover the collection, usage, disclosure, and storage of personal information. They allow individuals to access their personal information, and have it corrected if it is incorrect. The 13 APPs are as follows:

APP 1 — 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.

APP 2 — Anonymity and pseudonymity

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

APP 3 — 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.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

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

APP 6 — Use or disclosure of personal information

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

APP 7 — Direct marketing

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

APP 8 — Cross-border disclosure of personal information

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

APP 9 — 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.

APP 10 — 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.

APP 11 — 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.

APP 12 — 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.

APP 13 — Correction of personal information

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

3. Australian Privacy Principles Privacy Policy

The RTO's only collects personal information about an individual to fulfil an obligation under AVETMISS standards, State, or independent funding body requirements, or to undertake normal business activity (such as correspondence, meet legal obligations or respond in an emergency). All information that is gathered is provided by the individual concerned and can only be accessed by nominated or authorised staff members. This information cannot be made available to any other organisation or individuals except where:

- The individual would reasonably expect the APP entity to use or disclose the information related to the primary purpose of training
- The disclosure of the information is required or authorised by Australian law, court order, or a permitted health situation
- The APP entity reasonably believes disclosure of personal information is necessary for enforcement related activities by an enforcement body

The types of organisations to which personal information is disclosed

- Government departments such as Australian Skills Quality Authority (ASQA), State Funding Departments, The Australian Taxation Office, Centrelink, and Job Network Agencies
- To an employer or organisation sponsoring a student's study
- To the parent or authorised representative of a student who is a minor (under 18)
- Other tertiary educational institutions for results, course completion or certificate verification to facilitate an application to that institution

Individuals have the right to access own information and have explained how information is collected, stored, and used for transparency.

Information Security: (Principle 4)

All reasonable steps are taken to ensure the information collected is protected from misuse, loss, and is safe from unauthorised access, modification, or disclosure. Information no longer required will be destroyed or stored securely (if a requirement of other legislation, or as required by the Public Records Office). Information held in student files that are being used or are being held outside of the secure storage area will always be under the control of an authorised member of staff.

Openness: (Principle 5)

Individuals will be provided everything about the way personal, sensitive and health information is managed. This information will be available to anyone who asks, regarding the sort of personal sensitive and health information held and for what purpose, how it is collected, used, and disclosed.

Access and Correction: (Principle 6)

We will provide individuals with access to information, or the opportunity to correct information held. Under some circumstances, personal information will not be corrected, in which the reasons will be made clear and the individual requesting the change of information will have access to a complaint handling procedure.

Anonymity: (Principle 8)

Individuals have the option of not identifying themselves unless identification is required by law or is practical. No educational services can be offered unless the student freely identifies themselves therefore student anonymity is not an option. No transfer of personal information is allowed unless required by law.

Procedures

The business collects and stores personal information on our students and industry clients. We comply with the Privacy Act. This procedure describes how personal information is collected, managed, used, disclosed, protected, and disposed in accordance with the APPs.

1. Authority to collect and store information

Approved Registered Training Organisation by the Australian Skills Quality Authority, in which registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires collection of personal and sensitive information from students. This requirement is specified in the Data Provision Requirements 2011 which is one of five legislative instruments that must complied with as a condition of registration.

The data provision requires collection of data from students in accordance with the Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS). This defines information about the student, where training is delivered, what they are studying and the mandatory reporting of training activity to government agencies. Together these requirements form an obligation to collect, store and report information of any student participating in nationally accredited training.

2. Collection and use

Collection of personal information, directly or indirectly, is only necessary for delivery and support of the services offered. Some of the information collected is ‘sensitive’ as defined by the Privacy Act and can be broadly categorised as follows:

Solicited information

- Contact information such as name, organisation, position, address, telephone, and email are collected for marketing, student support services, mandatory reporting and for communicating with relevant stakeholders as part of our day-to-day operation

- Additional information includes training activity, storage and reporting information relating to satisfaction surveys and complaint handling
- Names, addresses, phone numbers, emergency contact details, bank account details and other employment related information is collected from employees for the purpose of managing human resources. The management of staff personal information complies with this business process.

Collection methods

- Student personal and sensitive information as well as training activity information is prescribed by the AVETMIS Standard. This information is collected directly from our students using enrolment forms which may be paper based or electronic and other administrative forms including but not limited to complaint forms, recognition application, request for refund, transfer application etc. Much of this information is entered into our Student Management System. Hard copy records are retained within a student file for a pre-determined timeframe before securely destroyed.
- Survey responses are collected using Employer and Student Satisfaction Surveys which are issued in electronic format. Returned surveys are imported directly into the Student Management System
- Enquiries from prospective students including personal contact information is collected directly from individuals who make data requests either by telephone, email, in person, or via our website
- Staff personal information is collected prior to start of employment

Sensitive information

Personal information collected that may be regarded as 'sensitive' under the Privacy Act includes:

- Disability and long-term impairment status (health), Indigenous status, Language spoken at home, Proficiency in spoken English and Country of birth. This information is specified in the AVETMISS data elements and is collected for the national VET data collections and surveys and may be collected for VET-related research.

Direct marketing

Individual's right are respected to not receive marketing material, communications, and dissemination of personal information in accordance with APP 7 (Direct marketing), the Spam Act, and the Do Not Call Register Act. It is not a practice to cold call individuals for the purpose of marketing services. All contact from the marketing team is initiated by the student or potential student. Contact details are only provided by individuals where they have initiated an enquiry.

Google Analytics and cookies

Websites automatically collect personal information when you are browsing or using our websites. The information collected includes:

- The server and IP (Internet Protocol) address of the machine that has accessed the website
- The dates and times of each visit to the website
- The pages accessed and documents downloaded
- The type of browser used
- Sometimes the previous site visited

Unsolicited personal information

Unsolicited personal information will be treated and managed according to the APPs.

Notification of collection

Aim is to notify an individual of collected personal information before, at the time, or as quickly as possible thereafter. Notification are usually electronic but may be verbal.

Disclosure of personal information

Personal information is not disclosed other than for the purpose for which it was collected, unless the individual has consented, or would reasonably expect personal information to be communicated such as required by law. In these circumstances reasonable steps should be taken to inform the individuals concerned and seek consent with personal information handled according to the APPs.

There is no selling of mailing lists to third parties for marketing purposes.

There is no disclose of personal information overseas. While people around the world can access material published on our website, no statistical or research publications contain identifiable personal information.

Management of personal information

Personal information collected, used, or disclosed is to be accurate, up to date, complete and relevant. Updated information is routinely captured by the Student Management System as we are advised of changes.

Access to and correction of personal information

Individuals may subject to exceptions, request access to and correction of their personal information. There is no charge for giving access to or for correcting personal information.

Requests for access to or correction of personal information should be made by emailing the RTO and a response will be sent within 14 business days.

Information retention and disposal

Personal information is held in electronic and paper format:

- Information collected from student enrolment applications and survey responses is held in databases
- Names and contact details of students, trainers, employers, and staff are held in the Student Management System and Zoho a CRM for employers
- Names and contact details collected during the delivery of services may be held either in electronic form or paper which are held securely on premises
- Personal staff information is retained by parent company Angus Knight
- Backup copies of all electronic files held in systems are kept in the event of system failure or loss. All backup copies of system files are secured.

Personal information is retained as prescribed by regulating and funding bodies. Certification documentation is retained for 30 years. When personal information is no longer necessary, and lawful to do so it will be securely destroyed.

Information security

Active steps are taken to protect personal information from misuse, interference, loss, unauthorised access, and modification or disclosure.
Systems and network are protected from unauthorised access using appropriate technologies. The inherent risks associated with data transmission over the internet are acknowledged. Mailing of information is an option if security concerns exist. Appropriate technologies include the following:

- Access to Student Management System is protected through user log-on and password, and assignment of user access rights
- Third-party providers used for the delivery of services are all located within Australia and are required to be compliant with the APPs and offer appropriate safeguards to protect personal information
- Main premises and data storage systems are fully secured. A clean-desk business practice is in place and sleep mode locks workstations when not in use. Paper documents containing names

and addresses are locked away and shredded when destroyed. All hardware is properly 'sanitised' before disposal.
- Two-factor identification required for VPN access from home
- Security training is regularly provided, active testing identifies security weakness such as phishing
- Laptops screened to identify if able to access the network, security updates occur within a day, USBs are not able to access the network, and TeamViewer utilised to access Angus Knight IT support

Complaints and concerns

Complaints or concerns about the management of personal information should be directed in writing to the General Manager in line with the Complaints and Appeal Policy and Process.

Related Policies and Procedures

- All Policies and Procedures

Responsible Officer

The responsible officer for the implementation of this Policy is the General Manager

Publishing details

Document Name	Privacy Policy and Procedure
Approved by	General Manager
Date of Approval	1-09-2022
Version	3
Summary of content (new) or amendments (revised)	New policy, all changes will be captured in the Continuous improvement and Version Control Registers
Next Review Date	1-09-2023