POL001 Privacy Policy

SHAFSTON
SCHOOL OF BUSINESS

Privacy Policy and Procedure

This policy sets out how Shafston International Pty Ltd (including its registered business names Shafston International College and Shafston School of Business), referred to in this document as "Shafston", collects, holds, uses, discloses, secures and manages personal and sensitive information in accordance with applicable privacy law, including the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth).

This policy applies to all personal and sensitive information collected by Shafston in relation to students, personnel, contractors, and other stakeholders. It covers all methods of information handling, including digital, physical, and verbal communications.

Shafston is committed to protecting the privacy of individuals and ensuring the confidentiality, security, and integrity of personal and sensitive information. The organisation will comply with the Australian Privacy Principles and other relevant legislation while fostering trust and transparency in all interactions.

Shafston complies with the *Privacy Act 1988* (Cth) *including the* 13 Australian Privacy Principles (APPs) as outlined in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). Providing an overall framework for our privacy practices, Shafston has developed and implemented this APP Privacy Policy.

Personal information includes 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.

For example, personal information may include:

- An individual's name, signature, address, phone number or date of birth,
- Sensitive information,
- Credit information,
- Employee record information,
- Photographs,
- Internet protocol (IP) addresses,
- Voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique), and
- Location information from a mobile device (because it can reveal user activity patterns and habits).

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, and
- Some aspects of biometric information.

Rationale

Shafston 's privacy processes are designed to support effective and compliant privacy practices by aligning with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs). These processes ensure that personal and sensitive information is managed responsibly, transparently, and securely, fostering trust among stakeholders while meeting regulatory obligations. By outlining clear procedures for the collection, use, storage, and disclosure of information, Shafston ensures that all activities are compliant with national and state-specific legislation. This includes robust measures for maintaining data quality and security, such as password-protected ICT systems, secure physical storage, and regular audits to prevent unauthorised access, misuse, or loss of personal information.

The organisation demonstrates transparency through accessible privacy policies, detailed notifications at the point of data collection, and clear avenues for individuals to request access to or correction of their personal information. Provisions for anonymity and informed consent further respect individual privacy, while processes for handling complaints and escalating unresolved issues to external authorities reinforce accountability. Regular monitoring and evaluation of privacy practices enable continuous improvement, ensuring that processes remain effective and adapt to evolving legal and organisational requirements. Together, these comprehensive privacy processes safeguard individual rights and promote organisational integrity.

Legislation

The following legislation applies according to Shafston 's activities, locations and statutory coverage:

- *Privacy Act 1988 (Cth),*
- *Privacy Regulations 2025 (Cth),*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth),
- *Education Services for Overseas Students Act 2000* (Cth),
- *Information Privacy Act 2014* (ACT),
- *Health Records (Privacy and Access) Act 1997 (ACT),*
- *Listening Devices Act 1992 (ACT),*
- *Workplace Privacy Act 2011 (ACT),*
- *Privacy and Personal Information Protection Act 1998* (NSW),
- *Health Records and Information Privacy Act 2002 (NSW),*
- *Surveillance Devices Act 2007 (NSW),*
- *Workplace Surveillance Act 2005 (NSW),*
- *Information Act 2002 (NT),*
- *Surveillance Devices Act 2007 (NT),*
- *Information Privacy Act 2009* (QLD),
- *Invasion of Privacy Act 1971 (QLD),*
- *Surveillance Devices Act 2016 (SA),*
- *Personal Information Protection Act 2004* (TAS),
- *Listening Devices Act 1991 (TAS),*
- *Privacy and Data Protection Act 2014 (VIC),*
- *Health Records Act 2001 (VIC),*
- *Surveillance Devices Act 1999 (VIC),*
- *Privacy and Responsible Information Sharing Act 2024 (WA), and*
- *Surveillance Devices Act 1998 (WA).*

Australian Privacy Principles

Shafston 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 code and provide suitable procedures for Shafston personnel to be able to deal with related inquiries and complaints that may be received from time to time.

The following sections of this policy outline how we manage personal information.

Australian Privacy Principle 1 Open and transparent management of personal information

Purposes for information collection, retention, use and disclosure

Shafston retains a record of personal information about all individuals with whom we undertake any form of business activity. Shafston must collect, hold, use and disclose information from our clients and stakeholders for a range of purposes, including but not limited to:

- Providing services to clients,
- Managing employee and contractor teams,
- Promoting products and services,
- Conducting internal business functions and activities, and
- Requirements of stakeholders.

As a government registered training organisation, regulated by the Australian Skills Quality Authority, Shafston is required to collect, hold, use and disclose a wide range of personal and sensitive information on students in nationally recognised training programs. This information requirement is outlined in the *National Vocational Education and Training Regulator Act 2011* (Cth) and associated legislative instruments. In particular, the legislative instruments:

- *Student Identifiers Act 2014* (Cth),
- *National Vocational Education and Training Regulator (Outcome Standards for NVR Registered Training Organisations) Instrument 2025* (Cth),
- *National Vocational Education and Training Regulator (Compliance Standards for NVR Registered Training Organisations and Fit and Proper Person Requirements) Instrument 2025* (Cth),
- *Higher Education Support Act 2003* (Cth), and

- *Data Provision Requirements 2020* (Cth).

It is noted that Shafston is also bound by various State Government Acts requiring similar information collection, use and disclosure (particularly *Education Act(s), Vocational Education and Training Act(s) and Traineeship and Apprenticeships Act(s)* relevant to state jurisdictions of Shafston operations).

It is further noted that, aligned with these legislative requirements, Shafston delivers services through a range of Commonwealth and State Government funding contract agreement arrangements, which also include various information collection and disclosure requirements.

Individuals are advised that due to these legal requirements, Shafston discloses information held on individuals for valid purposes to a range of entities including:

- Governments (Commonwealth, State or Local),
- Apprentice Connect Australia Providers,
- Employers (and their representatives), Job Network Providers, Schools, Guardians, and
- RTOs such as RTO Management Services for data management, credit agencies and background check providers.

Kinds of personal information collected and held

The following types of personal information are generally collected, depending on the need for services delivery:

- Contact details,
- Employment details,
- Educational background,
- Demographic Information,
- Course progress and achievement information, and
- Financial billing information.

The following types of sensitive information may also be collected and held:

- Identity details,
- Employee details and HR information,
- Complaint or issue information,
- Disability status and other individual needs,
- Indigenous status, and
- Background checks (such as National Criminal Checks or Working with Children checks).

Where Shafston collects personal information of more vulnerable segment of the community (such as children), additional practices and procedures are also followed. Please refer to Shafston 's **Child Safety and Wellbeing Policy** further information.

How personal information is collected

Shafston 's usual approach to collecting personal information is to collect any required information directly from the individuals concerned. This may include the use of forms (such as registration forms, enrolment forms or services delivery records) and the use of web-based systems (such as online enquiry forms, web portals or internal operating systems).

Shafston does receive solicited and unsolicited information from Third party sources in undertaking services delivery activities. This may include information from such entities as:

- Governments (Commonwealth, State or Local),
- Apprentice Connect Australia Providers,
- Employers (and their representatives), Job Network Providers, Schools, Guardians, and
- RTOs such as credit agencies and background check providers.

How personal information is held

Shafston 's usual approach to holding personal information includes robust storage and security measures at all times. Information on collection is:

- As soon as practical converted to electronic means,
- Stored in secure, password protected systems, such as financial system, learning management system and student management system, and
- Monitored for appropriate authorised use at all times.

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role. Shafston ICT systems are hosted internally with robust internal security to physical server locations and server systems access. Virus protection, backup procedures and ongoing access monitoring procedures are in place.

Destruction of paper-based records occurs as soon as practicable in every matter, through the use of secure shredding and destruction services at all Shafston sites. Individual information held across systems is linked through an Shafston allocated identification number for each individual.

Retention and Destruction of Information

Shafston maintains a *Retention and Disposal Schedule* documenting the periods for which personal information records are kept. Specifically, for our RTO records, in the event of our organisation ceasing to operate the required personal information on record for individuals undertaking nationally recognised training with us would be transferred to the Australian Skills Quality Authority, as required by law.

Use of AI

Our Privacy Policy and collection notices explain our use of AI, the kinds of personal information processed by AI, purposes of use, sources, disclosures, generation/inference, any overseas processing, and how to contact us about AI.

Shafston maintains an AI Register identifying approved AI products and features, their purposes, relevant information categories, suppliers, access permissions, authorised users and privacy risk assessments. The Privacy Officer oversees the register and reviews it when products, functionality or information-handling arrangements change.

The organisation defines permitted and prohibited uses of each AI product, provides role-appropriate training on privacy and security risks, continuously monitor outputs for accuracy and drift, and conducts regular audits of AI use.

aXcelerate is beta testing an AI assistant feature. Shafston treats any proposed use of this feature as subject to approval and AI Register controls, including review of privacy, vendor access, information processing and output accuracy. AI-generated suggestions or summaries may assist an assessor but must not be treated as evidence of competency or as an assessment judgement. All competency decisions are made and recorded by an appropriately qualified Shafston assessor, who independently reviews the learner's evidence against the unit requirements. AI must not independently determine a learner's assessment outcome, competency, certification or progression.

Automated decisions

Shafston reviews computer-supported processes before use, including beta features, and whenever their purpose, information inputs or role in decision-making changes. The Privacy Officer records the review and ensures the AI Register and this policy reflect actual approved practices.

From 10 December 2026, where Shafston uses personal information in a computer program that makes a decision, or does something substantially and directly related to making a decision, which could reasonably be expected to significantly affect an individual's rights or interests, this policy will identify the kinds of personal information used and the kinds of decisions made solely by, or substantially and directly supported by, the program. Shafston will assess its actual system configuration and use against this requirement before that date and whenever functionality changes.

This review includes rules-based software, spreadsheets and AI; a human making the final decision does not automatically remove the disclosure obligation. It covers beneficial and adverse outcomes, including refusing or failing to make a decision.

Individuals can contact the Privacy Officer to ask about these uses, request access to or correction of personal information, or raise a concern through the existing privacy complaints procedure.

The Privacy Officer obtains sufficient information from system owners and suppliers to keep these disclosures meaningful and current. Sensitive information categories are identified where used; general AI labels and collection notices do not replace these privacy-policy disclosures.

Accessing and seeking correction of personal information

Shafston confirms all individuals have a right to request access to their personal information held and to request its correction at any time. In order to request access to personal records, individuals are to make contact with:

Shafston Privacy Officer

Peter Wei – peter.wei@shafston.com

A number of third parties, other than the individual, may request access to an individual's personal information. Such third parties may include employers, parents or guardians, schools, Apprentice Connect Australia Providers, Governments (Commonwealth, State or Local) and various other stakeholders.

In all cases where access is requested, Shafston ensures that:

- Parties requesting access to personal information are robustly identified and vetted,
- Where legally possible, the individual to whom the information relates will be contacted to confirm consent (if consent not previously provided for the matter), and
- Only appropriately authorised parties, for valid purposes, will be provided access to the information.

Complaints about a breach of the APPs or a binding registered APP code

If an individual feels that Shafston may have breached one of the APPs or a binding registered APP code, please refer to the *Privacy Complaints Procedure* below for further information on what actions may be taken.

Likely Overseas Access and Disclosure of Personal Information

Shafston operates in an international education environment. Authorised overseas contractors located in China and Indonesia may access personal information in Shafston's approved student management system, aXcelerate, for approved administration and student support activities. Providing personal information to these overseas contractors may constitute overseas disclosure under Australian Privacy Principle 8.

This access is provided for legitimate operational purposes, including student administration, enrolment processing, student support, course management and other activities directly related to Shafston's education and training services.

Overseas access to personal information is restricted to authorised personnel who require the information to perform their duties. Shafston implements appropriate privacy and information security measures, including role-based access permissions, secure system authentication, confidentiality obligations and monitoring of system access.

Where personal information is disclosed to an overseas recipient, Shafston takes reasonable steps to ensure the information is handled in accordance with the Australian Privacy Principles (APPs), as required by the *Privacy Act 1988 (Cth)*.

The countries currently identified for overseas contractor access and potential disclosure are China and Indonesia. Shafston will take reasonable steps to ensure overseas contractors handle personal information consistently with the Australian Privacy Principles, including through appropriate contractual, access-control and security arrangements. Any additional likely overseas recipient countries will be identified and this policy updated where practicable.

Shafston remains committed to protecting the confidentiality, integrity and security of personal information, regardless of the geographical location from which it is accessed.

Making our APP Privacy Policy available

Shafston makes this APP Privacy Policy available free of charge through the privacy section of its website [https://business.shafston.edu/privacy-policy/]. The policy is provided in accessible formats on reasonable request. In addition, this policy is:

- Prominently displayed at each Shafston 's premises,
- Included within our **Student Handbook**,
- Noted within the text or instructions at all information collection points (such as informing individuals during a telephone call of how the policy may be accessed, in cases where information collection is occurring), and

- Available for distribution free of charge on request, as soon as possible after the request is received, including in any particular format requested by the individual as is reasonably practical.

If, in the unlikely event the APP Privacy Policy is not able to be provided in a particular format requested by an individual, we will explain the circumstances around this issue with the requester and seek to ensure that another appropriate method is provided.

Review and Update of this APP Privacy Policy

Shafston reviews this APP Privacy Policy:

- On an ongoing basis, as suggestions or issues are raised and addressed, or as government required changes are identified,
- Before production use of any new AI product or any material change in how an existing AI product processes personal information,
- Through our internal audit processes on at least an annual basis,
- As a part of any external audit of our operations that may be conducted by various government agencies as a part of our registration as an RTO or in normal business activities, and
- As a component of each and every complaint investigation process where the compliant is related to a privacy matter.

Where this policy is updated, changes to the policy are widely communicated to stakeholders through internal personnel communications, meetings, training and documentation, and externally through publishing of the policy on Shafston 's website and other relevant documentation (such as our *Student Handbook*) for clients.

Australian Privacy Principle 2 Anonymity and pseudonymity

Shafston provides individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with us in relation to a particular matter, whenever practical. This includes providing options for anonymous dealings in cases of general course enquiries or other situations in which an individuals' information is not required to complete a request.

Individuals may deal with us by using a name, term or descriptor that is different to the individual's actual name wherever possible. This includes using generic email addresses that does not contain an individual's actual name, or generic usernames when individuals may access a public component of our website or enquiry forms.

Shafston only stores and links pseudonyms to individual personal information in cases where this is required for services delivery (such as system login information) or once the individual's consent has been received.

Individuals are advised of their opportunity to deal anonymously or by pseudonym with us where these options are possible.

Requiring identification

Shafston must require and confirm identification however in services delivery to individuals for nationally recognised course programs. We are authorised by Australian law to deal only with individuals who have appropriately identified themselves. That is, it is a *Condition of Registration* for all RTOs under the *National Vocational Education and Training Regulator Act 2011* that we identify individuals and their specific individual needs on commencement of services delivery and collect and disclose Australian Vocational Education and Training Management of Information Statistical Standard (AVETMISS) data on all individuals enrolled in nationally recognised training programs. Other legal requirements, as noted earlier in this policy, also require considerable identification arrangements.

There are also other occasions also within our services delivery where an individual may not have the option of dealing anonymously or by pseudonym, as identification is practically required for us to effectively support an individual's request or need.

Australian Privacy Principle 3 — Collection of solicited personal information

Shafston only collects personal information that is reasonably necessary for our business activities.

We only collect sensitive information in cases where the individual consents to the sensitive information being collected, except in cases where we are required to collect this information by law, such as outlined earlier in this policy.

All information we collect is collected only by lawful and fair means. We only collect solicited information directly from the individual concerned, unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

Where an AI product generates or infers personal information, Shafston treats this as collection. We limit such activity to what is reasonably necessary, ensure lawful and fair means, prefer direct collection where practicable, and obtain consent before generating or inferring any personal or sensitive information.

Australian Privacy Principle 4 Dealing with unsolicited personal information

Shafston may from time to time receive unsolicited personal information. Where this occurs, we promptly review the information to decide whether or not we could have collected the information for the purpose of our business activities. Where this is the case, we may hold, use and disclose the information appropriately as per the practices outlined in this policy.

Where we could not have collected this information (by law or for a valid business purpose) we immediately destroy or de-identify the information (unless it would be unlawful to do so).

Australian Privacy Principle 5 Notification of the collection of personal information

Whenever Shafston collects personal information about an individual, we take reasonable steps to notify the individual of the details of the information collection or otherwise ensure the individual is aware of those matters. This notification occurs at or before the time of collection, or as soon as practicable afterwards.

Our notifications to individuals on data collection include:

- Shafston 's identity and contact details, including the position title, telephone number and email address of a contact who handles enquiries and requests relating to privacy matters,
- The facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a Third party, including the name of that party,
- If the collection is required or authorised by law, including the name of the Australian law or other legal agreement requiring the collection,
- The purpose of collection, including any primary and secondary purposes,
- The consequences for the individual if all or some personal information is not collected,
- Other organisations or persons to which the information is usually disclosed, including naming those parties,
- Whether we are likely to disclose the personal information to overseas recipients, and if so, the names of the recipients and the countries in which such recipients are located.
- A link to this APP Privacy Policy on our website or explain how it may be accessed, and
- Advice that this APP Privacy Policy contains information about how the individual may access and seek correction of the personal information held by us, and how to complain about a breach of the APPs, or any registered APP code, and how we will deal with such a complaint.

Where possible, we ensure that the individual confirms their understanding of these details, such as through signed declarations, website form acceptance of details or in person through questioning.

Collection from third parties

Where Shafston collects personal information from another organisation, we:

1. Confirm whether the other organisation has provided the relevant notice above to the individual, or
2. Whether the individual was otherwise aware of these details at the time of collection, and
3. If this has not occurred, we will undertake this notice to ensure the individual is fully informed of the information collection.

Australian Privacy Principle 6 Use or disclosure of personal information

Shafston only uses or discloses personal information it holds about an individual for the particular primary purposes for which the information was collected, or secondary purposes in cases where:

- An individual consented to a secondary use or disclosure,
- An individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection, or
- Using or disclosing the information is required or authorised by law.

For VET data system contractor access under section 6 of the National Vocational Education and Training Regulator (VET Data System Information) Determination 2026, the Privacy Officer confirms that the information was collected

under the Data Provision Requirements or equivalent requirements in a non-referring State, and that the handling facilitates that reporting. The handling must relate to contracted design, build, operation, maintenance or testing of the relevant system and comply with the contract.

For a relevant contract entered into after section 6 commenced on 8 September 2026, Shafston confirms that the contractor is contractually obliged to comply with the Australian Privacy Principles as if it were an APP entity for the covered information. The review includes subcontractors within the Determination's definition. This specific condition does not apply retrospectively to earlier contracts.

Before relying on this authorisation, the Privacy Officer records the applicable purpose, information, contractor and contractual protection. Access is limited to the approved work; unrelated reuse is not authorised by this Determination. Existing privacy, security and incident controls continue to apply. Ordinary ICT support is not automatically a training or assessment third-party arrangement.

AI use and disclosure test

Before any personal information is entered into, shared with or processed by any AI product, Shafston requires a documented check that this use matches the original collection purpose, or is within reasonable expectation for any secondary purpose, or is directly related if sensitive information is involved.

If this cannot be confirmed, Shafston obtains consent from the individual prior to AI use.

Requirement to make a written note of use or disclosure for this secondary purpose

If Shafston uses or discloses personal information in accordance with an 'enforcement related activity' we will make a written note of the use or disclosure, including the following details:

- The date of the use or disclosure,
- Details of the personal information that was used or disclosed,
- The enforcement body conducting the enforcement related activity,
- If the organisation used the information, how the information was used by the organisation, and
- The basis for our reasonable belief that we were required to disclose the information.

Australian Privacy Principle 7 Direct marketing

Shafston does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, unless:

- The personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing, or
- The personal information has been collected from a Third party, or from the individual directly, but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing, and
- We provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

On each of our direct marketing communications, Shafston provides a prominent statement that the individual may request to opt out of future communications, and how to do so. An individual may also request us at any stage not to use or disclose their personal information for the purpose of direct marketing, or to facilitate direct marketing by other organisations. We comply with any request by an individual promptly and undertake any required actions for free.

We also, on request, notify an individual of our source of their personal information used or disclosed for the purpose of direct marketing unless it is unreasonable or impracticable to do so.

Australian Privacy Principle 8 Cross-border disclosure of personal information

Before Shafston discloses personal information about an individual to any overseas recipient, we take reasonable steps to ensure that Shafston does not breach any privacy matters in relation to that information.

Personal information in aXcelerate may be accessed remotely by approved personnel in the following countries (this statement does not establish that aXcelerate hosts or stores data in those countries):

- China
- Indonesia

Australian Privacy Principle 9 Adoption, use or disclosure of government related identifiers

Shafston does not adopt, use or disclose a government related identifier related to an individual except:

- In situations required by Australian law or other legal requirements,
- Where reasonably necessary to verify the identity of the individual,
- Where reasonably necessary to fulfil obligations to an agency or a State or Territory authority, or
- As prescribed by regulations.

Australian Privacy Principle 10 Quality of personal information

Shafston takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. We also take reasonable steps to ensure that the personal information we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. This is particularly important:

- When we initially collect the personal information, and
- When we use or disclose personal information.

We take steps to ensure personal information is factually correct. In cases of an opinion, we ensure information takes into account competing facts and views and makes an informed assessment, providing it is clear this is an opinion. Information is confirmed up to date at the point in time to which the personal information relates.

Quality measures in place supporting these requirements include:

- Internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training personnel in these practices, procedures and systems),
- Protocols that ensure personal information is collected and recorded in a consistent format, from a primary information source where possible,
- Requiring AI input validation and output verification where AI systems include the use or creation of personal information,
- Ensuring updated or new personal information is promptly added to relevant existing records,
- Providing individuals with a simple means to review and update their information on an on-going basis through our online portal,
- Reminding individuals to update their personal information at critical services delivery points (such as completion) when we engage with the individual,
- Contacting individuals to verify the quality of personal information where appropriate when it is about to be used or disclosed, particularly if there has been a lengthy period since collection, and
- Checking that a third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems.

Where personal information is sourced from or transformed by AI, records are labelled as “AI-derived.” Shafston personnel verify the accuracy and relevance of data before relying on such information for decisions or actions that affect individuals.

Shafston informs individuals when AI is used in ways that may materially affect them.

Australian Privacy Principle 11 — Security of personal information

Shafston takes active measures to consider whether we are able to retain personal information we hold, and also to ensure the security of personal information we hold. This includes reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

We destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

Access to Shafston offices and work areas is limited to our personnel only visitors to our premises must be authorised by relevant personnel and are accompanied at all times. With regard to any information in a paper-based form, we maintain storage of records in an appropriately secure place to which only authorised individuals have access.

Regular personnel training and information bulletins are conducted with Shafston personnel on privacy issues, and how the APPs apply to our practices, procedures and systems. Training is also included in our personnel induction practices.

We conduct ongoing internal audits (at least annually and as needed) of the adequacy and currency of security and access practices, procedures and systems implemented.

Australian Privacy Principle 12 — Access to personal information

Where Shafston holds personal information about an individual, we provide that individual access to the information on their request. In processing requests, we:

- Ensure through confirmation of identity that the request is made by the individual concerned, or by another person who is authorised to make a request on their behalf,
- Respond to a request for access:
  - Within 14 calendar days, when notifying our refusal to give access, including providing reasons for refusal in writing, and the complaint mechanisms available to the individual, or
  - Within 30 calendar days, by giving access to the personal information that is requested in the manner in which it was requested.
- Provide information access free of charge.

Australian Privacy Principle 13 Correction of personal information

Shafston takes reasonable steps to correct personal information we hold, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

Individual Requests

On an individual's request, we:

- Correct personal information held, and
- Notify any third parties of corrections made to personal information, if this information was previously provided to these parties.

In cases where we refuse to update personal information, we:

- Give a written notice to the individual, including the reasons for the refusal and the complaint mechanisms available to the individual,
- Upon request by the individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading,
- Respond within 14 calendar days to these requests, and
- Complete all actions free of charge.

Correcting at Shafston 's initiative

We take reasonable steps to correct personal information we hold in cases where we are satisfied that the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading (that is, the information is faulty). This awareness may occur through collection of updated information, in notification from third parties or through other means.

AI Governance and Assurance

Shafston may use approved AI products and features to support administration, learning and assessment activities. Shafston maintains an AI Register for oversight of approved products, functionality and information-handling risks. The controls below apply where personal information is involved.

APP 1 and 5: Transparency

This policy and relevant collection notices explain approved AI use, including categories of personal information processed, purposes, any generation or inference, relevant disclosures and overseas processing where applicable. The AI Register identifies the products and features approved for use and their purposes.

APP 3: Collection, generation and inference

AI-generated or inferred personal information is treated as collection. Shafston limits such activity to what is reasonably necessary, ensure lawful and fair means, prefer direct collection where practicable, and obtain consent before generating or inferring sensitive information.

APP 6: Use and disclosure

Before any personal information is processed by an AI product, Shafston personnel complete an APP 6 assessment of primary purpose match or reasonable expectation for any secondary purpose, including direct relation for any sensitive information.

Processing does not proceed unless these requirements are satisfied of further consent is obtained.

APP 10: Accuracy and oversight

Records that include AI-derived personal information are labelled as "AI derived." Personnel verify accuracy and relevance before use that may affect an individual. We inform individuals where AI is used in ways that may materially affect them.

Lifecycle assurance

Shafston maintains policies that define permitted and prohibited uses of AI, provide role-based training, monitor outputs, and perform regular audits of AI use.

Recording and Monitoring

Shafston approves recording and monitoring only where it supports learning, accessibility, safety or another authorised business purpose and privacy risks can be controlled.

These requirements apply to on-site, online and placement activities, regardless of who owns the equipment. They cover:

- Audio, video, screen and call recording, including phones, cameras, CCTV and wearables.
- Live streaming, transcription, location tracking, sensors and AI processing.
- Local and offline use, connected devices, applications, accounts and remote services.

Personal health and assistive functions are considered individually. Ordinary non-electronic eyewear is outside scope. Possession of a device alone does not establish recording or misconduct.

Approval

The CEO or documented delegate provides written approval before recording other people or organisational information, streaming, transcription, organisational tracking or cloud AI processing.

The approval identifies the purpose, functions, users, locations, configuration, accounts, recipients, retention period and review date. Routine recordings may have standing approval with specified operators, settings and notices. Publication, security monitoring and AI reuse require separate approval.

Host permission, general enrolment consent or approval of a device does not authorise every function. Local display and audio-output uses receive proportionate consideration.

The activity owner records the privacy assessment in existing risk and planning records, including:

- The benefit, less intrusive options and advice needed on privacy, security, safety, accessibility or assessment.
- How information is collected, viewed, stored, synchronised, shared, processed overseas and deleted, including vendor access, transcripts and backups.

A formal privacy impact assessment is required for high-risk proposals and where required by law. Unresolved legal or technical risks prevent approval.

The activity owner checks controls before use and after material changes:

- Use necessary functions, supported software, secure accounts, restricted access and approved storage.
- Use RTO-managed equipment and accounts for organisational recording wherever practicable.
- Disable personal backups, social posting, vendor AI training and other secondary uses unless separately assessed and lawfully approved.

An indicator light or network block alone does not confirm that recording or uploading is disabled.

CCTV approval specifies the system owner, purpose, camera coverage, audio settings, signage, protected areas, authorised viewers, access logs and footage-request process. It does not authorise teaching, assessment or personnel-performance use.

For online meetings, calls and screen recording, approval covers participant locations, administrators, recording destinations, downloads and transcription bots. New audio, bot access or purposes require review before use.

Notices and Agreement

The Quality Manager confirms requirements for each location and records required permissions, notices, consultation and restrictions. Unresolved requirements are referred for specialist advice before use.

For planned private audio or video sessions, Shafston obtains express, specific agreement from affected participants and provides an accessible collection notice explaining:

- The active functions, purpose, recipients and remote attendees.
- Cloud or AI processing, retention, access, complaint contacts and alternatives.

Agreement must be voluntary, informed, current and given with capacity. Attendance, silence, indicator lights and general publicity releases are insufficient. Applicable legal consent, workplace notice and prohibition requirements also apply.

For children, the responsible person considers capacity, the child's views and required parent or guardian involvement. An adult relative is not automatically authorised to consent for another adult.

Publicity is optional and separate from learning. If consent is refused or withdrawn, future consent-based recording or use stops and an alternative is considered. Explain any lawful retention or legal hold; later consent does not remedy unlawful recording.

Personal Devices and Accessibility

Personnel and students disclose proposed recording, streaming, transcription, tracking and AI functions before use. Approval identifies the equipment, software, accounts, storage, destinations, updates and incident arrangements.

Use managed equipment or another method if organisational information cannot be separated and controlled. Report loss, accidental recording, unexpected synchronisation or sharing promptly. Approval does not authorise access to unrelated personal content, personal passwords, confiscation or whole-device wiping.

Reasonable adjustments are considered confidentially through existing student support or personnel processes. Consult the user, consider alternatives and record conditions, reasons and review options. A person need not disclose disability publicly. An assistive purpose does not authorise every recording, cloud or AI function.

Conditions of Use

Shafston prohibits:

- Routine covert recording, continuous personal ambient recording and public streaming from placements.
- Learner biometric identification or emotion scoring, and AI-only competency decisions.
- Recording in toilets, changing areas, intimate-care or similarly protected settings.

Ordinary approval cannot override these prohibitions. Equipment must meet safety, PPE, hygiene and site requirements. Check education and care placement restrictions before attendance; switching off a device may not satisfy a possession restriction.

For each approved session, the activity owner ensures:

- Before use: settings and recipients are checked, unrelated information is removed from view, and notices, permissions and alternatives are confirmed.
- During use: active functions and a pause signal are explained. Recording stays within the task and stops for breaks, newcomers, objections, sensitive information, unsafe conditions or unexpected functions until resolved.
- After use: remote access ends, records transfer through the approved route, unexpected synchronisation is checked and temporary links are revoked. Disposal follows retention and incident requirements.

Placements and Assessment

The placement coordinator confirms host monitoring, including fixed systems, software and personal devices. The placement agreement records purpose, functions, notices, permissions, site restrictions, supervision, evidence access, retention and incident responsibilities.

Host approval does not replace individual rights or Shafston 's duties. Students can report directly to Shafston and receive an alternative activity where recording cannot proceed safely or lawfully.

Assessors specify permitted assistance and adjustments, verify identity and evidence authenticity, and check assessment conditions and off-camera assistance. Footage, AI summaries and any aXcelerate AI assistant outputs do not replace assessor judgement. Only an appropriately qualified assessor can determine competency after independently reviewing relevant and sufficient evidence. Obtain further evidence where needed and use existing integrity and appeal processes fairly; approved adjustments are not cheating.

Records

Apply the Retention and Disposal Schedule, relevant contracts, public-records requirements and legal holds to recordings, transcripts and summaries according to their purpose. Record provenance, permitted use and access restrictions. Not all raw footage is assessment evidence or a certification record.

The activity owner verifies disposal across devices, cards, platforms, backups, approved storage and vendors. Access, correction and complaints follow this policy's existing procedures.

Incidents and Review

For unapproved or accidental recording, personnel:

- Protect people, stop recording or transmission where safe, restrict access through authorised systems and promptly notify the manager and Quality Manager.
- Record facts, functions, accounts, recipients and actions without unnecessarily circulating recordings.
- Use lawful, proportionate authority for personal-device access and evidence preservation. Refer suspected illegal imagery through safeguarding or police channels without routine viewing, copying or forwarding.

The response lead assesses privacy, safety, safeguarding, assessment, employment and host obligations and applies the relevant notification requirements without delay. Unapproved use is not automatically a notifiable breach; lack of organisational knowledge does not resolve responsibility.

Preserve lawful protected disclosures, abuse reporting and emergency assistance. Seek specialist advice on disputed exceptions before disciplinary or disclosure decisions.

The activity owner reviews benefits, accessibility, consent, incidents, technical reliability, support costs and controls before expanding a pilot. Material changes to purpose, location, settings, software, recipients, AI functions, vendor terms or legal requirements require reapproval.

The Quality Manager monitors legislative commencement dates, including Commonwealth automated-decision transparency from **10 December 2026** and WA notifiable information breach requirements from **1 January 2027**.

Request for Records Access

Individuals or third parties may at any stage request access to records held by Shafston relating to their personal information. The following procedure is followed on each individual request for access:

1. A request for access is provided by the requester, with suitable information provided to be able to:
    a. Identify the individual concerned,
    b. Confirm their identity, and
    c. Identify the specific information that they are requesting access to.
2. This request may be in any form, or preferably using Shafston 's *Records Access or Update Request Form*.
3. Upon receiving a request for access, Shafston then:
    a. Confirms the identity of the individual or party requesting access,
    b. Confirms that this individual or party is appropriately authorised to receive the information requested,
    c. Searches the records that we possess or control to assess whether the requested *personal information* is contained in those records, and
    d. Collates any personal information found ready for access to be provided.

Confirming identity

Shafston personnel must be satisfied that a request for personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf. The minimum amount of personal information needed to establish an individual's identity is sought, which is generally an individual's name, date of birth, last known address and signature.

When meeting the requesting party in person, identification may be sighted.

If confirming details over a telephone conversation, questions regarding the individual's name, date of birth, last known address or service details must be confirmed before information is provided.

4. Once identity and access authorisation is confirmed, and personal information is collated, access is provided to the requester within 30 calendar days of receipt of the original request. We will provide access to personal information in the specific manner or format requested by the individual, wherever it is reasonable and practicable to do so, free of charge.

   Where the requested format is not practical, we consult with the requester to ensure a format is provided that meets the requester's needs.

5. If the identity or authorisation access cannot be confirmed, or there is another valid reason why Shafston is unable to provide the personal information, refusal to provide access to records will be provided to the requester, in writing. Our notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual. Such notifications are provided to the requester within 30 calendar days of receipt of the original request.

Request for Records Update

Individuals or third parties may at any stage request that their records held by Shafston relating to their personal information be updated. The following procedure is followed on each individual request for records updates:

1. A request for records update is provided by the requester, with suitable information provided to be able to:
   i. Identify the individual concerned,
   ii. Confirm their identity, and
   iii. Identify the specific information that they are requesting be updated on their records.

   This request may be in any form, or preferably using Shafston 's *Records Access or Update Request Form*.
2. Upon receiving a request for records update, Shafston then:
   i. Confirms the identity of the individual or party to whom the record relates,
   ii. Searches the records that we possess or control to assess whether the requested *personal information* is contained in those records, and
   iii. Assesses the information already on record, and the requested update, to determine whether the requested update should proceed.

   Assessing Update

   Shafston personnel assess the relevant personal information we hold, and the requested updated information, to determine which version of the information is considered accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

   This may include checking information against other records held by us, or within government databases, in order to complete an assessment of the correct version of the information to be used.
3. Once identity and information assessment is confirmed, personal information is:
   a. Updated, free of charge, within 14 calendar days of receipt of the original request, and
   b. Notified to any third parties of corrections made to personal information, if this information was previously provided to these parties.
4. If the identity of the individual cannot be confirmed, or there is another valid reason why Shafston is unable to update the personal information, refusal to update records will be provided to the requester in writing, free of charge, within 14 calendar days.

   Our notification will include the reasons for the refusal and the complaint mechanisms available to the individual.

5. Upon request by the individual whose correction request has been refused, we will also take reasonable steps to associate a 'statement' with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading. This statement will be applied, free of charge, to all personal information relevant across Shafston systems within 30 calendar days of receipt of the statement request.

Privacy Complaints

If an individual feels that Shafston has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. We encourage individuals to discuss the situation with their Shafston representative in the first instance, before making a complaint.

The complaints handling process is as follows:

1. The individual should make the complaint including as much detail about the issue as possible, in writing to Shafston :

   Peter Wei – peter.wei@shafston.com

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

3. After considering this response, if the individual is still not satisfied, they may escalate their complaint directly to the Information Commissioner for investigation:

   Office of the Australian Information Commissioner

   www.oaic.gov.au

   Phone: 1300 363 992

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

4. 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:

   Australian Skills Quality Authority

   www.asqa.gov.au

   Phone: 1300 701 801

Monitoring and Evaluation

Shafston monitors and evaluates privacy processes to ensure effectiveness.

A process of performance monitoring, evaluation, and reporting has been established and implemented.

The organisation continually improves the effectiveness and efficiency of processes. Process performance and outcomes are regularly audited to identify and remove causes of existing and potential problems, as well as to uncover any opportunities for improvement.

Please refer to the **Quality Policy** for further information on the monitoring and evaluation process.