Government of Western Australia
South Regional TAFE

Policy – Privacy (website version)

Policy Owner: Director Capability People & Culture
Subject Expert: Reporting and Business Services Manager (Privacy Officer)
Version: 2
Date approved: 2/11/2026
Next review date: 9/10/2028

---

1. Purpose

South Regional TAFE (SRTAFE) respects an individual's right to privacy and is committed to managing personal information responsibly, transparently, and in accordance with the Privacy Act 1988 (Cth) and the Privacy and Responsible Information Sharing Act 2024 (WA).

2. Scope

This policy applies to all information (including sensitive personal information) SRTAFE collects, stores, uses and discloses about:

- people using its services (including students, clients and people registering for services); and
- people who work, or apply to work, for SRTAFE (including employees, secondees, volunteers, work experience staff/students, contractors, sub-contractors, vendors, and service providers).

It also applies to information sharing between SRTAFE and other stakeholders:

- other government entities, whether Commonwealth, State, or Local.
- contracted service providers.
- non-government entities.

3. Principles

SRTAFE collects and retains personal information relating to individuals involved in its training, operational, and business activities to support its core functions and services.

It does this in accordance with the Information Privacy Principles (IPPs) listed in the Privacy and Responsible Information Sharing Act 2024 which outline how personal information must be handled for all IPP entities including SRTAFE.

3. Procedures

These guiding procedures explain how South Regional TAFE (SRTAFE) will deliver its services and activities which require the collection, use and storage of personal and sensitive information in accordance with legislated requirements.

Types of personal information collected and held
Personal and sensitive information will only be collected where it is necessary for our delivery of service and activities, regulatory or enforcement functions, or either required or authorised by or under law or the individual consents to the collection of the information.

Accordingly, SRTAFE will collect the least amount of personal information necessary to deliver its functions and activities.
Additional safeguards are used in recognition that these types of personal information are particularly sensitive.

The types of personal information collected, depending on which functions or activities, can include but is not limited to:

- Contact details (e.g. name, phone number, email, address and postal address).
- Personal circumstances (e.g. age, gender, occupation, education history, parent or guardian details, emergency contacts, language).
- Financial information (e.g. payment details, bank account details, and credit history).
- Identity information (e.g. date of birth, signatures, citizenship, and visa status).
- Employment information (e.g. employment status and work history, referee comments, and salary).
- Government identifiers (e.g. tax file number).
- Other information voluntarily provided by an individual (e.g. survey responses or competitions or other events).

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

- Images and audio (e.g. photographs and video, and voice recordings). This includes closed circuit television (CCTV) video and audio recordings.
- Government related identifiers which may include, but is not limited to:
    - Unique Student Identifier (USI).
    - Tax File Numbers for VET Student Loans and employment taxation purposes.
    - Citizenship and residency documents.
    - Concession details.
    - Birth Certificate, driver's licence or passport to establish identity.
- Employee details and Human Resources information.
- Complaint or feedback information.
- Health information about an individual.
- Racial or ethnic origin.
- Religious affiliation.
- Political opinions or associations.
- Background checks (such as National Criminal Checks or Working with Children checks).

Notification of the collection of personal information
SRTAFE takes reasonable steps to notify individuals, or to make them aware, of the collection of their personal information. Notification or awareness is provided at or before the time the information is collected, or, where that is not practicable, as soon as reasonably practicable afterwards.

This includes notification where personal information may be shared without consent under authorised responsible information sharing arrangements, and the circumstances in which this may occur.

How personal information is collected

Only a student's personal information necessary for training delivery will be collected directly from the individual or their authorised representative when:

- Applying and enrolling with SRTAFE.
- Completing any application form in person, by phone or by email.
- Submitting information via SRTAFE's website.

As an employee or prospective employee, specific details may be obtained by contacting our People and Culture team for Recruitment purposes, Remuneration payment (banking details), and/or Performance Management.

Personal information may also come from third parties such as associated commercial partners and social media sites.

Website

If an individual is browsing SRTAFE's website or social networking services:

- Personal information is not collected however systems may record certain information about use of the website.
- The Western Australian Department of Training and Workforce Development (DTWD) which manages the SRTAFE website does not attempt to collect a visitor's Personal Information. A person can generally visit the website without revealing Personal Information, unless they choose to provide it.
- The information collected by the DTWD is dependent upon the actions undertaken when visiting the website.
- SRTAFE may use "cookies" which is a piece of information delivered to and stored by your web browser when you access information from certain websites. DTWD may use cookies from time to time to improve user experience.
- The following information may be automatically recorded by the website's web server for statistical and system administration purposes:
    - the user's server address
    - the user's top-level domain name (eg .gov, .com, .au, .nz etc)
    - the type of browser used to access the site
    - the date and time the user accessed the site
    - the pages accessed and the files downloaded
    - the referring website

This information assists DTWD to understand how the website is used and helps to keep improving information quality.

If an individual follows a link from the SRTAFE website to a third-party website or links that allows shared content, these third-party links may facilitate collection of information through this interaction (this may occur indirectly). Please read the privacy statement of the relevant third-party websites and options they may make available to individuals in relation to collection of personal information.

Marketing collection

Talent Release Forms

Talent Release Forms (TRFs) must be completed by students, contractors, and other external stakeholders.

A TRF is required for each campaign where external talent is engaged. Prior to completion of the TRF, the Marketing team will clearly communicate to the talent how, where, and for how long their footage or still imagery will be used, ensuring the talent is able to provide

informed consent.

Personal information collected through a TRF may include the talent's name, email address, telephone number, and signature. Where the talent is under the age of 18, the personal information of a parent or guardian is also collected, including their name, email address, telephone number, and signature. The TRF also provides an option for the talent to opt out of having their name used in association with the imagery or footage.

All personal information collected via TRFs is stored securely within a secure Teams folder and moved into a folder within Content Manager once completed. Access is restricted to authorised personnel only.
Department of Training and Workforce Development will require students to complete their own TRF. This also applies to any other agency that wishes to take photos of current students, they will be requesting permission from the student or legal guardian.

Personal information will not be shared with any other external agencies or businesses without the explicit consent of the talent.

Direct marketing (Electronic Direct Mail - EDMs)
SRTAFE will not use or disclose personal information for the purpose of direct marketing (EDMs) unless the information has been collected from an individual who could reasonably expect it to be used for marketing purposes.
All EDMs sent on behalf of SRTAFE must include a clear and accessible opt-out option at the time of distribution, in accordance with the Spam Act 2003.
Requests to opt out of EDMs must be actioned within five (5) business days by SRTAFE.
However, individuals cannot opt out of receiving administrative messages in relation to any course in which they are currently enrolled.

Compulsory collection of personal information
As a Government registered training organisation, regulated by the Training Accreditation Council (TAC) WA, SRTAFE is required to collect, hold, use and disclose a wide range of personal and/or sensitive information (including third parties) 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:

- Student Identifiers Act 2014 (Cth)
- National Vocational Education and Training Regulator Act 2011 (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)
- Data Provision Requirements 2020 (Cth).
- Vocational Education and Training Act 1996 (WA)
- The Vocational Education and Training (General) Regulations 2009 (WA)
- Registration Standards 2025 (WA)

Anonymity and non-disclosure
There may be lawful or practicable circumstances, such as general enquiries and some

reporting instances, where an individual may remain anonymous or use an alias or assumed name. The use of a pseudonym does not necessarily mean that an individual cannot be identified.

There are many circumstances where, for various reasons, including legislative requirements, anonymity is not possible. For example, it might not be practical to deal with an individual anonymously when processing a payment, delivering goods or services, communicating personally or when required or authorised by law or a court/tribunal order to deal with identified individuals.

If an individual chooses not to provide personal information to SRTAFE for the purposes set out in this procedure, they may not be able to enrol in courses or receive or access certain products and services.

Uses and disclosure of personal information
Primary and secondary purposes may include, without limitation, use of an individual's personal information to:

- Allow SRTAFE to answer individual's enquiries.
- Process any application for enrolment or employment with SRTAFE.
- Verify an individual's identity.
- Inform another agency of a change of address.
- Conduct statistical and/or regulatory student surveys. Individuals may opt out of any survey at the time they are contacted.

SRTAFE uses personal information for the primary purpose for which it is collected and for secondary purposes that are either:

- Reasonably related to the primary purpose; or
- Authorised or required by law, including under responsible information sharing arrangements.
- Explicitly described elsewhere in the Privacy Policy and Procedures.

An individual's health and/or sensitive information may be used to:

- Ensure any education programs in which they participate are run safely and in accordance with any special health needs requirements.
- For insurance purposes; or
- Otherwise as required or authorised under an Australian law or legislation.

<u>Consent to share</u>
SRTAFE may collect, use, or disclose personal and sensitive information without an individual's consent where such collection, use, or disclosure is authorised or required by law, including under Privacy and Responsible Information Sharing Act 2024.
Responsible information sharing may occur where it is necessary to promote the safety, wellbeing, or public interest of an individual or group, or to enable SRTAFE to perform its statutory and regulatory functions.
When making decisions to share information under this section, SRTAFE will apply the following principles:

- Necessity – only information that is reasonably necessary for the intended purpose will be shared.
- Proportionality – the amount and sensitivity of information shared will be proportionate to the risk or issue being addressed.

- Least intrusive means – de-identified information will be used where practicable.
- Accountability – decisions to share information will be documented and subject to internal oversight.

De-identified information

SR TAFE may use de-identified personal or sensitive information to prepare submissions to government or a government body or plan events and activities. Re-identification of personal information will only occur where the information is required or authorised by law or for specific purposes to provide services.

Third parties

In some circumstances SRTAFE may need to use or disclose personal and/or sensitive information (including third parties) where required to do so by law or due to statistical, legislative/regulatory authority and research requirements which include, but not limited to:

- Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS). Fact sheets.
  Personal information that will be included in the National VET Provider Collection may be used or disclosed in accordance with the National VET Data Policy.
- VET Student Loans applications (www.studyassist.gov.au)
- School (if enrolled in a school-based apprenticeship or traineeship or are a Vocational Education and Training Delivered to Secondary Students student (VETDSS)).
- Employer (if enrolled with SRTAFE as an apprentice or trainee).
- Parent/guardian if under the age of 18 (unless an individual has formally advised SRTAFE not to provide this information).
- Government authorities and agencies.
- Organisations conducting student surveys. Individuals may opt out of any survey at the time they are contacted.
- Researchers.
- Required to investigate an unlawful activity.
- Required by an enforcement body for investigative activities.
- Necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.
- SRTAFE professional advisers, accountants, auditors and lawyers or insurer.

CCTV

We use CCTV to deliver services safely and securely through deterrence and investigation of any safety or security incidents on any campus and any land we own or control.
We will disclose CCTV recordings to law enforcement bodies for investigation activities, legal advisers, insurers, and courts for liability claims and prosecutions.

Information sharing agreements

SRTAFE supports responsible information sharing and will ensure compliance with legislative requirements.
Information sharing arrangements and agreements will be limited to authorised recipients and subject to appropriate safeguards to prevent misuse, unauthorised access, or further disclosure.
SRTAFE will conduct an initial Privacy Threshold Assessment to all proposed agreements. If any high impact function or activity is identified, then a Privacy Impact Assessment is required under the PRIS Act. Further information can be found on the WA Gov website.

Storage and security of personal information
SRTAFE takes steps to ensure that any record containing personal and sensitive information is protected by security safeguards as reasonable in the circumstances to take against loss, unauthorised use, modification or disclosure and misuse.
Security measures include:

- physical controls, such as secure office premises and locked storage.
- electronic controls, including passphrase protection, encryption, and firewalls.
- access controls, to restrict information to authorised personnel only.
- staff training in information security and privacy obligations.
- regular audits and monitoring of information systems.

SRTAFE does not utilise third-party data storage providers that may store personal information in other countries.

SRTAFE maintains compliance to the WA Government Cyber Security policy, and State Records Act that outlines required retention periods for personal information records.

Managing access to personal information
SRTAFE establishes strong governance processes and secure system controls to ensure personal information is accessed only in authorised and appropriate ways.
Access to personal information is granted solely to employees who require it to perform their duties, consistent with the least-privilege principle, meaning staff receive only the minimum level of access necessary for their role.

SRTAFE implements role-based permissions, secure authentication measures, and audit logging to ensure that all access is controlled, monitored, and traceable.
Access rights are regularly reviewed and adjusted to ensure they remain appropriate, including the removal of access when staff change roles or no longer require it.

Physical records containing personal information are stored in secure, access-controlled environments to prevent unauthorised viewing, handling, or removal.
All employees are required to follow established procedures and undertake mandatory training to ensure personal information is handled safely, responsibly, and in accordance with SRTAFE's privacy obligations.

Privacy breaches and incident management
SRTAFE takes reasonable steps to identify, manage, and respond to suspected or actual data breaches involving personal or sensitive information.
SRTAFE maintains a Data Breach Response Plan which outlines roles, responsibilities, escalation pathways, and mitigation actions in the event of a data incident.

In the event of an actual or suspected privacy breach (i.e., unauthorised access to, or unauthorised disclosure of, personal information held by SRTAFE), SRTAFE will take the necessary steps to contain the breach and remediate it in line with its breach management procedures.
Any unauthorised disclosure or misuse of personal information will be managed under the SRTAFE Code of Conduct.

Where a breach involves personal information and is reasonably likely to result in serious harm, SRTAFE will notify affected individuals and relevant authorities, as a matter of best

practice and in accordance with law.

Dealing with unsolicited personal information
SRTAFE may receive unsolicited personal information. Unsolicited personal information is personal information received by SRTAFE where SRTAFE has taken no active steps to collect the information (e.g., misdirected mail; petition; an employment application on an individual's own initiative and not in response to an advertised vacancy; promotional flyer promoting an individual's business or services, etc.).

Any unsolicited personal details received will be afforded appropriate privacy protection, even where SRTAFE has not solicited the personal information. Should SRTAFE determine if any unsolicited personal information could not have been collected, SRTAFE will destroy or de-identify the personal information if it is lawful or reasonable to do so.

Automated decisions
SRTAFE does not engage in automated decision making using personal information. Any decisions relating to students, staff, or other individuals are made through human review and assessment rather than computer generated processes.

Unique identifiers
Is an identifier (usually a number) that is used for the purpose of identifying an individual. SRTAFE may assign unique identifiers where necessary to support the efficient delivery of its functions - such as internal staff numbers, student identifiers or system generated reference numbers. These are treated as personal information when an individual can be reasonably identified from them.
SRTAFE collects, uses and discloses unique identifiers only for the purpose for which they were created, for a related purpose that an individual would reasonably expect, or where required or authorised by law.
SRTAFE takes reasonable steps to protect all unique identifiers from misuse, loss, unauthorised access, modification or disclosure.

Disclosure of personal information outside Australia
SRTAFE does not disclose personal information to recipients outside Australia.

Access and seek correction of personal information
All students and staff of SRTAFE can access their personal information held by SRTAFE at no charge unless SRTAFE is authorised to refuse access by an Act, law or a court/tribunal order. Alternatively, under the Freedom of Information Act 1982.
Access to reprints of an individual's academic transcript and/or Award incurs fees as per the VET Fees and Charges Policy as published.

SRTAFE will endeavour to collect, use and disclose personal information that is accurate, complete and up to date. SRTAFE will verify the accuracy and currency of an individual's personal information at each subsequent engagement with the individual, particularly if there has been a lengthy period since collection.

Individuals are encouraged to notify SRTAFE of any changes to their personal information to assist in maintaining data accuracy. If an individual believes their personal information is inaccurate, incomplete, or out of date they are to contact SRTAFE to take reasonable steps to ensure the information is corrected.

Privacy complaints
A complaint can be submitted by using the online Feedback form found on the SRTAFE website. Refer to the SRTAFE Policy and Procedure for Complaints for more detailed information on how to lodge a complaint and how complaints are managed by SRTAFE. All complaints are taken seriously and investigated promptly in a confidential manner. If the complaint is not resolved to an individual's satisfaction, they may contact the Office of the Information Commissioner Western Australia.

Contact details
If you have any questions about this privacy policy or how we handle personal information or wish to make an access or correction request email our Privacy Officer at: privacy@srtafe.wa.gov.au.

5. Related policies and other supporting documents

5.1 Policies

- Recordkeeping
- Confidentiality
- Client Complaints & Feedback
- Information Classification
- Information Security Management Delegations
- Information Systems Security

5.2 Associated procedures

- Privacy
- Record Management
- Information Classification
- Client Complaint & Feedback

5.3 Additional documents

- Privacy Statement (Website version)
- Privacy and Responsible Information Sharing (PRIS) and South Regional TAFE Values
- Important Terms & Conditions of Enrolment
- Staff Code of Conduct

6. Definitions and acronyms

Personal information - includes name, date of birth, address, contact information, location information, unique identifiers (e.g. drivers licence number or IP address), information that relates to someone's features or behaviour. It can include personal information about a deceased person and inferences made about people. This list is not exhaustive.

Sensitive personal information - includes information that relates to an individual's racial or ethnic origin, gender identity, sexual orientation, political opinions, religious beliefs, trade union membership, or criminal record. It also includes health, genetic or genomic and biometric information. This list is not exhaustive.

De-identified information - is information that has been changed or had information removed so that an individual can no longer be identified from it.

Disclosure - is sharing personal information outside the IPP entity.

6. Policy governance

Privacy and Responsible Information Sharing Act 2024 (WA)

Freedom of Information Act 1992 (WA)

State Records Act 2000 (WA)

Office of Information Commissioner WA

Privacy Act 1988

Privacy Amendment (Enhancing Privacy Protection) Act 2012

Australian Privacy Principles (APP)

Freedom of Information Act 1982

AVETMISS Collection Protocols

Spam Act 2003

National VET Data Policy

Office of the Australian Information Commissioner

Chapter 1: Privacy complaint handling process | OAIC

7. Document version control

See version history of this document in Doc Hub.