

DOCUMENT REFERENCE:	PPP046
RESPONSIBLE COMMITTEE:	Executive Team
CATEGORY:	Governance
APPROVED DATE:	September 2025
DATE OF NEXT REVIEW:	September 2027
RELATED DOCUMENTS:	Legislation: Privacy and Data Protection Act (<i>amended</i>) 2014 (Vic) Privacy Act 1988 (Commonwealth) Student Identifiers Act 2014 (Commonwealth) Health Records Act 2001 Freedom of Information Act 1982 VPDSF Protective Data Security Plan Public Record Office Victoria Victorian Public Records Act 1973 Documents: PPP047 Privacy Statement PPP186 Integrity Framework PPP213 Records Retention and Disposal Guideline

1. Introduction

South West TAFE (SWTAFE or the 'Organisation') complies with the Victorian *Privacy and Data Protection Act 2014 (PDPA)*, the *Commonwealth Privacy Act 1988* and the *Health Records Act 2001* and adheres to the privacy principles outlined in these Acts.

2. Definitions

Disclose	the disclosure by us to a third party
Individual	a natural person
Third Party	a third party other than us or an individual
Personal Information	information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of: • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not.
Use	the internal use of personal information by us

3. Privacy Statement

We have a Privacy Statement PPP047 that outlines how we will treat personal information. It is available on request, at Reception at each campus and via our website.

4. Collection of data

We will not collect personal information about an individual unless the information is necessary for one or more of our functions or activities. Our collection of personal information will be fair, lawful and not intrusive. Where we collect personal information, we will declare:

- the purpose of the collection
- how the information will be used
- how the individual can get access to that information, and
- what happens if the individual does not provide the information

Information will be stored within SWTAFE approved systems.

5. Use

Personal information will only be used for:

- the primary purpose for which it was collected
- a secondary purpose that the individual could reasonably expect
- any purpose for which the individual has provided explicit consent

We may be required by legislation or funding agreements to collect and report certain data on behalf of the Government or other agencies.

6. Disclosure

We will only disclose personal information for the purpose for which it was collected. Where a request is made by a party other than the individual to obtain, use or share information about the individual, then we will not do so unless we have sought permission in writing from the individual concerned.

We are not required to seek permission, to use or disclose personal information in circumstances related to public interest, such as law enforcement and public or individual health and safety. Whilst we take reasonable steps to ensure third parties handle data appropriately, we cannot guarantee their compliance once data is disclosed.

In accordance with the Privacy and Data Protection Act 2014, sections 15A (*Family Violence Protection Act 2008*) and 15B (*Child Wellbeing and Safety Act 2005*), we are required to disclose personal information to the relevant authorities.

7. Data quality

We take reasonable steps to ensure that the personal information we collect, use or disclose is accurate, complete and up-to-date. Data accuracy is maintained through regular reviews and by allowing users to update their information as needed.

8. Data and Information security

We take reasonable steps to protect the personal information we hold from misuse, loss, and unauthorised access, modification, or disclosure.

At times, it may be necessary to take personal information off-site in order to fulfil our responsibilities—for example, when visiting students in their workplaces or marking assessments. In such cases, only the necessary documentation is taken, and all reasonable precautions are followed to safeguard the information.

Documents must not be left unattended in view. If unattended, they must be secured in a locked container, such as a filing cabinet or secured bag.

9. Anonymity

We give people the option to interact anonymously whenever it is lawful and practicable to do so. An anonymous interaction might be appropriate when an individual is providing feedback or making a complaint about a service without wishing to be identified

10. Access and correction

We provide an individual with access to their personal information upon written request and proof of identification. Where an individual can show that the information held about them is not accurate, current or complete, we will take reasonable steps to correct that information. Some requests for access or amendment to information held by us will need to be made under the *Freedom of Information (FOI) Act 1982*. Charges for FOI access are governed by the Freedom of Information Act, its amendments and regulations.

Unless being accessed under the Freedom of Information Act, access to any personal information held about an individual is provided to them free of charge. We may choose to charge a fee to make a copy of personal information. Should a fee apply, it will not be excessive and the cost incurred will be disclosed prior to preparation of the information.

11. Identifiers

Where a person is required to provide us with their unique identifier from another agency (*such as Centrelink*) we will not adopt this identifier as our own.

We only assign unique identifiers to individuals where it is necessary in order to carry out one or more of its functions or activities. Our Student ID is created for this purpose. We will not make this unique identifier available to others unless obligated by Government or another agency to pass on this information as an element of data reporting.

We are obliged to abide by the Student Identifiers Act 2014, and must collect, record and report a student's USI to Government upon enrolment into their qualification and/or application for a VET Student Loans

12. Transborder data flows

We only transfer personal information to a recipient in another state or a foreign country in circumstances where the information will have appropriate protection.

13. Sensitive information

We will not collect sensitive personal information unless the individual has consented, or it is required by law, or where there are other special circumstances such as those relating to health services provision and individual or public health or safety.

14. Personal Information Storage

We store personal information in secure environments located both within Australia and overseas. Our preference is to use Australian-based data centres that demonstrate robust security practices and compliance with relevant privacy legislation.

Where data is stored overseas, we take all reasonable steps to identify the country of storage, maintain a register of these locations, and ensure that appropriate safeguards are in place. This includes assessing the provider's compliance with international data protection standards and contractual obligations.

We use a combination of on-premises systems and cloud-based services to support our operations. All cloud providers are subject to due diligence checks to ensure they meet our security and privacy requirements. Where feasible, data is encrypted both at rest and in transit to protect against unauthorised access.

We are committed to maintaining the confidentiality, integrity, and availability of personal information and regularly review our data governance practices to ensure ongoing compliance with applicable laws and standards.

15. Record Keeping

We are committed to protecting personal information and ensuring compliance with Victorian privacy and records management obligations. Our recordkeeping practices are governed by the Privacy and Data Protection Act 2014 (Vic) and the Public Records Act 1973 (Vic).

We manage records, including documents, emails, databases, images, and recordings—in accordance with legal retention schedules to minimise privacy risks and uphold data integrity.

We adhere to the Retention and Disposal principles:

- Records are securely disposed of once they are no longer required, in accordance with the PPP213 Records Retention and Disposal Guideline
- Records containing personal information are retained only for the minimum period required under applicable Retention and Disposal Authorities (RDAs) issued by the Public Record Office Victoria (PROV)

16. Training

To ensure ongoing alignment with privacy legislation and best practices, SWTAFE requires all its staff to complete an annual privacy training to promote awareness and accountability.

17. Other Obligations

We comply with the Internet Industry Code of Practice regarding electronic information and other applicable codes of practice.

Our existing obligations under other laws, such as providing formal access to records under the Freedom of Information Act 1982 apply.

18. Breaches of this Policy

In the first instance, alleged privacy breaches should be referred to the area where the information was initially lodged by the individual.

If a satisfactory resolution cannot be reached at this level, the alleged breach should be submitted in writing to the Audit and Compliance Officer as our nominated Privacy Officer:

Privacy Officer
South West Institute of TAFE
P O Box 674
WARRNAMBOOL 3280
Email: feedback@swtafe.edu.au