



PRIVACY

MANAGEMENT

STRATEGY

Contents

1. INTRODUCTION	3
OVERVIEW	3
MANDATE AND COMMITMENT	3
Roles and Responsibilities.....	3
2. PRIVACY MANAGEMENT STRATEGY	5
2.1. PART 1 - COMMITMENT	5
2.2. PART 2 – PRACTICES	6
2.3. PART 3 – MONITORING	8
3. APPENDIX	9
3.1. DEFINITIONS	9
3.2. REFERENCES	10

1. INTRODUCTION

South West TAFE (SWTAFE) respects the privacy of everyone who interacts with us and is committed to protecting and managing personal information fairly and lawfully. This Privacy Management Strategy (the Strategy) is intended to provide an outline as to how SWTAFE implement good privacy practices. The Strategy encourages holistic privacy management by interconnecting a wide range information management tools.

OVERVIEW

SWTAFE has obligations regarding the collection, use and management of individuals' personal information under the **Privacy and Data Protection Act 2014 (Vic)** ("PDP") and the **Health Records Act 2001 (Vic)**. SWTAFE is also subject to the requirements of the **Privacy Act 1988** (Cth) and understands and accepts the Australian Privacy Principles (APPs) and the objects of those principles, together with Schedule 1 of the PDP which contains Information Privacy Principles (IPP's). The IPPs are the core of privacy law in Victoria and set the minimum standard for how Victorian public sector organisations should manage personal information.

SWTAFE has established a Privacy Management Strategy that aims to;

- develop and promote a culture that protects and respects private information.
- educate people within SWTAFE about information privacy obligations.
- monitor privacy compliance and support the development of systems and process that ensure privacy by design.
- outline obligations for responding to complaints about potential privacy breaches.

MANDATE AND COMMITMENT

SWTAFE is committed to complying with its obligations in respect of personal information under the **Privacy and Data Protection Act 2014 (Vic)** and the **Health Records Act 2001 (Vic)**. To the extent that they apply to our activities, SWTAFE is also subject to the requirements of the **Privacy Act 1988** (Cth).

ROLES AND RESPONSIBILITIES

CEO and members of the Institute Executive Team (IET)

- approve the Privacy Management Strategy, and be responsible for oversight of compliance with the SWTAFE's Privacy Guidelines and Privacy Statement.
- approve actions that support the implementation of the Strategy.
- receive periodic updates on the Privacy Management Strategy, and notification of privacy breaches, complaints and their outcomes, including any complaints which are considered to pose risk of legal action against SWTAFE.
- model best privacy practices and ensure respect for the privacy of individuals is core to all aspects of the SWTAFE's culture.

Privacy Officer

- assist in the development and implementation of the Privacy Management Strategy.
- respond to requests for information and receive all complaints.
- support South West TAFE staff and volunteers in understanding SWTAFE's requirements in the management of personal information.
- be responsible for the provision of information, investigation of privacy breaches and resolution of complaints made under the **Privacy and Data Protection Act 2014 (Vic)**

- Monitor and make recommendations for improvement of our organisational processes for the management of personal information, data and privacy requirements.
- Raise awareness of the role of the Privacy Officer
- Establish internal training programs to ensure that our staff are up to date and informed in privacy obligations and requirements.
- Assist with improvement of our organisational processes for the management of personal information, data and privacy requirements

Institute Leadership Team (ILT) will:

- model good privacy behaviour by demonstrating sound judgment in privacy matters
- comply with legislative requirements
- ensure privacy breaches and near misses are reported to the Privacy Officer and investigated,
- identify privacy risks
- ensure training is provided for staff.

Audit Risk and Compliance Department:

- develop, implement and continuously improve the Privacy management processes, in conjunction with the Privacy Officer
- identify compliance obligations and risks relating to privacy in conjunction with managers
- undertake Privacy Impact Assessments (PIA)
- raise awareness of and support the role of the Privacy Officer
- advise on integration of privacy risk management within relevant policies and procedures, and business processes
- support training for managers and SWTAFE Staff in regard to privacy
- develop mechanisms for reporting of privacy management to senior management and the Board,
- respond to requests for personal information made under the Privacy Act
- Monitor, review and respond to privacy incidents
- review strategy and Guidelines that set out privacy obligations in line with the ***Privacy and Data Protection Act 2014 (Vic) (PDP Act)***
- make recommendations for improvement of our organisational processes for the management of personal information, data and privacy requirements.
- Building capability, promotion for all staff

Information Technology Services will:

- ensure that access controls are developed, implemented, maintained and include appropriate logging
- proactively manage security to all data and information on the SWTAFE network from accidental and malicious access

Authorised SWTAFE Staff:

Where information is collected in relation to the employment of staff, such information may be used in an aggregated form for the purposes of financial, workforce planning or other employment related matters by staff authorised by SWTAFE to carry out such work.

All Staff

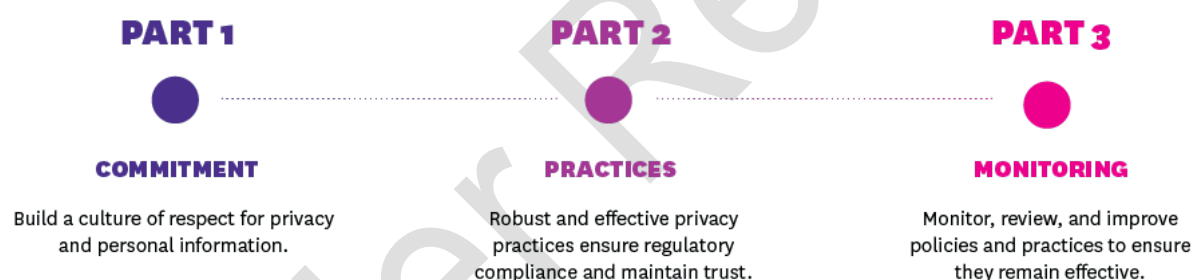
Every individual employee has responsibility for maintaining the privacy of every individual whether they are a work colleague, student, or visitor to our organisation.

All SWTAFE employees are expected to:

- model good privacy behaviour by demonstrating sound judgment in privacy matters
- comply with legislative requirements
- ensure privacy breaches and near misses are accurately recorded, reported to the Privacy Officer and investigated,
- identify privacy risks
- ensure training provided by SWTAFE is completed in a timely manner

2. PRIVACY MANAGEMENT STRATEGY

Implementing the measures outlined in this strategy will enable SWTAFE to be accountable for its information handling practices, and convey to others that it values and respects the privacy rights of individuals. The strategy will assist SWTAFE to demonstrate the steps it has taken to comply with the IPPs and section 20 of the Privacy and Data Protection Act 2014 (VIC) ("PDP Act"), and entrench a culture of privacy across the organisation. This strategy is divided into three parts:

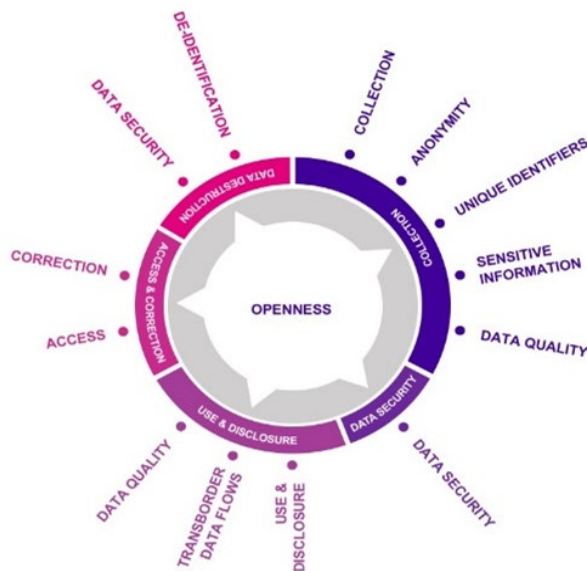


<https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-management-framework>

2.1. PART 1 - COMMITMENT

Building a culture of respect for privacy and personal information across SWTAFE starts with good privacy governance and leadership. South West TAFE have made a commitment to the following:

- SWTAFE ensures that its executive and senior management promote good privacy practices across the organisation. Using existing governance arrangements, such as board, executive committees and management meetings to raise privacy issues and create general privacy awareness creates an organisational culture that respects privacy.
- SWTAFE is aware and understands its privacy obligations and utilises the Office of the Victorian Information Commissioner's (OVIC) Guidelines to the Information Privacy Principles detail on how to interpret the IPPs in the PDP Act.
- SWTAFE has considered its privacy obligations under the Health Records Act 2001 (Vic), the Charter of Human Rights and Responsibilities Act 2006 (Vic), the Privacy Act 1988 (Cth).
- SWTAFE has appointed key roles and responsibilities for privacy management, including a member of staff with overall organisational accountability for privacy, managing day-to-day privacy, responsible for handling internal and external privacy enquiries, complaints, and providing advice to other staff on building privacy into their programs.



- SWTAFE will ensure appropriate resourcing is allocated to maintain organisational privacy expertise relative to its nature, size, and complexity.
- SWTAFE has ensured privacy is considered before, at the start of, and throughout the development and implementation of initiatives involving the collection, handling or use of personal information.
- SWTAFE has engaged with its legal representatives, finance, contract management, and project teams to build privacy into procurement, contract and project documentation.
- SWTAFE understands the role of OVIC and its approach to using regulatory powers to promote, assure and enforce the PDP Act.

SWTAFE has developed a four-phase action plan to implement the (OVIC) Guidelines to the Information Privacy Principles (IPP's)

2.2. PART 2 – PRACTICES

Robust and effective privacy practices ensure regulatory compliance maintain students and staff trust in SWTAFE's ability to handle personal information.

In order to uphold our compliance:

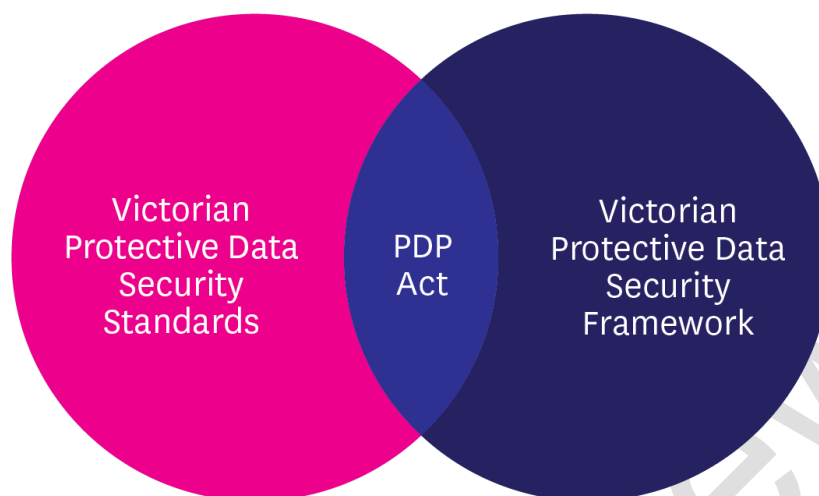
- SWTAFE has developed and maintains processes around handling personal information that align with the organisation's privacy obligations. An Information Privacy Policy and a Privacy Statement have been tailored to SWTAFE functions and activities it undertakes.
- SWTAFE maintains processes that covers the information lifecycle and clearly outlines staff responsibilities when handling personal information. The information lifecycle is the flow of information from the point the organisation collects the information to the point the information is destroyed.
The IPPs can be grouped into the five main stages of the information cycle as shown aside.

Figure 1: Information Cycle extract from:

<https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-full-text>

- SWTAFE will maintain PPP046 Information Privacy Policy and PPP047 Privacy Statement that is current, easily accessible, easy to understand, and accurately reflects the organisation's practices.
- SWTAFE maintains document PPP047 Privacy Statement which ensures reasonable steps are taken to give notice of the matters required under IPP 1.3 when collecting personal information. It is important to ensure steps taken to give notice (for example, a collection notice) are tailored to the circumstances, reviewed periodically, and consistent with the privacy policy.
- SWTAFE is aware of any information security obligations it has under the Victorian Protective Data Security Standards (VPDSS) and how the Victorian Protective Data Security Framework works in conjunction with the PDP & VPDSS.

Figure 2: Visual link of the interaction between Victorian Protective Data Security Standards (VPDSS), the Privacy & Data Protection Act 2014 and the Victorian Protective Data Security Framework



Extract from: <https://ovic.vic.gov.au/information-security/framework-vpdsf/>

- Privacy and security go hand-in-hand. Good information security practices protect personal information from unauthorised access, use, modification, or disclosure.
- SWTAFE will ensure it understands how and when personal information can be shared within and outside of the organisation, and how information should be protected when shared as outlined in the PPP046 Information Privacy Policy
- SWTAFE implement a risk management process that enables the organisation to identify, assess and manage privacy risks across the organisation. Risks should be added to the organisation's risk register, and an accountable person assigned to manage risks.
- SWTAFE has processes in place to ensure it monitors how long personal information should be retained before it is destroyed. Personal information must be destroyed or permanently de-identified when it is no longer needed for any purpose. Organisations should refer to the relevant Retention and Disposal Authority issued under the Public Records Act 1973 (Vic) when determining whether data should be destroyed or permanently de-identified.
- SWTAFE does incorporate privacy into staff inductions and conduct regular privacy training and awareness programs across the organisation.
- SWTAFE has a process for handling privacy enquiries and complaints. This information is easily accessible through its website to ensure stakeholders and the public can know who to contact within the organisation or where to get help.
- SWTAFE has developed a data breach response plan and an incident management process. We ensure staff know what to do and who to contact when a breach occurs.
- SWTAFE will review the implementation a program of engagement and awareness activities to build and enhance a privacy conscious culture. This will include staff participating in Privacy Awareness activities, or conducting regular seminars or other events with privacy officers and experts that highlight good privacy practices.

2.3. PART 3 – MONITORING

SWTAFE will monitor, review, and improve policies and practices to ensure they remain relevant and effective. Privacy is fast-moving and ever evolving which means SWTAFE needs to be proactive and anticipate future challenges which includes the following actions:

- SWTAFE will monitor and review its privacy policies and processes regularly to ensure they are up to date and fit for purpose. This will involve assessing its privacy documents to ensure they are up to date.
- SWTAFE will establish a process to measure or evaluate the effectiveness of the organisation's privacy practices, processes, and resources. This could include measuring the awareness of good privacy practices and the adoption and use of privacy tools or resources across the organisation.
- SWTAFE regularly reviews its risk register to ensure privacy risks are being appropriately managed.
- SWTAFE will proactively examine the privacy implications, risks and benefits of new technologies it introduces into the organisation, and address identified risks. Where a new process or technology changes the organisation's information handling practices, any privacy policies, collection notices and PIAs will be updated to reflect those changes.
- SWTAFE will ensure that any material changes to its privacy policies, procedures and practices are communicated appropriately to its employees and any relevant key stakeholders.
- SWTAFE does document compliance with its privacy obligations including keeping records of privacy process reviews, breaches and complaints. These records should enable an organisation to identify systemic privacy risks, common themes, and opportunities for improvement. Any themes and privacy risks identified should be reported to senior management and those responsible for privacy.
- SWTAFE will create a culture of continuous improvement by encouraging input from staff and key stakeholders with suggestions and feedback on the organisation's privacy practices.
- SWTAFE has its privacy processes assessed periodically by our independent internal auditor to identify areas that may need improvement.

3. APPENDIX

3.1. DEFINITIONS

Term	Definition
Australian Privacy Principles	means the set of 13 principles in the Privacy Act 1988 (Cth) governing the collection, quality, use, disclosure, management and transfer of personal information.
Health information	has the meaning given to it in section 3 of the Health Records Act 2001 (Vic) .
Health Privacy Principles	means the set of 11 principles in the Health Records Act 2001 (Vic) governing the collection, management, use, disclosure and transfer of health information by organisations such as South West TAFE.
Information Privacy Principles	means the set of 10 principles in the Privacy and Data Protection Act 2014 (Vic) governing the collection, use, disclosure, management and transfer of personal information by organisations such as South West TAFE.
Personal information	is any information, on its own or combined with other information, about an identifiable living individual.
Privacy by design	means a methodology to build privacy and data protection into the design and architecture of information systems, business processes and networked infrastructure.
Privacy impact assessment	means a risk analysis tool to identify and mitigate privacy and data protection risks, and to identify and evaluate privacy solutions.
Proactive privacy	means focusing on prevention rather than remediation.
Primary Purpose:	the purpose for which the information is collected. This is directly related to the core function or activity e.g. student enrolment.
Secondary Purpose:	when the information is used for another purpose than the primary purpose. The secondary purpose for which the information is collected must be connected or associated with the primary purpose. If sensitive information is involved, it must be directly related to the primary purpose.
Sensitive information	Information or an opinion about an individual including, but not limited to: - Racial or ethnic origin - Political opinions - Membership of a political association - Religious beliefs or affiliations - Philosophical beliefs - Membership of a profession or trade association - Membership of a trade Union - Sexual preferences or practices - Criminal record - Health information - Contact details - Employee or student performance

3.2. REFERENCES

- Privacy and Data Protection Act 2014 (Vic)
- Office of the Victorian Information Commissioner's (OVIC) Guidelines to the Information Privacy Principles
- Victorian Protective Data Security Framework
- PPP046 Information Privacy Policy
- PPP047 Privacy Statement
- Risk Management Procedure