Protecting Personal Information – the Privacy Fundamentals

STATE RECORDS
of South Australia

Government of South Australia
State Records

Contents

Acronyms

DPC	Department of the Premier and Cabinet Responsible for the Information Privacy Principles Instruction and Information Sharing Guidelines, and the provision of ICT, digital and cyber security support for South Australian government agencies.
EU	European Union An international organisation comprising 27 countries and governing comment economic, social and security policies.
FOI	Freedom of Information The right of the public to access information the government holds.
GDPR	General Data Protection Regulation A regulation that sets rules around the collection and processing of personal information.
ICT	Information and Communications Technology The use of telecommunication and computing technologies, tools and systems to support the creation, collection, processing, transmitting and storing of information.
IPPI	Information Privacy Principles Instruction Governs the collection, storage, use and disclosure of personal information collected by South Australian government agencies.
ISG	Information Sharing Guidelines Guidelines designed to give providers of services to children, young people and adults, confidence in sharing information to prevent harm or respond to current threats to safety and wellbeing.
PbD	Privacy by Design An approach that incorporates good privacy practices into decision making.
PIA	Privacy Impact Assessment A tool used to identify, assess and minimise privacy risks when managing personal information in relation to a specific project, program or system.
PMP	Privacy Management Plan A plan that identifies specific, measurable privacy goals and targets, and sets out how to achieve them.
PSMF	Protective Security Management Framework Describes the arrangements and expectations for personnel, physical and information security in South Australian government agencies.
SACSF	South Australian Cyber Security Framework Addresses cyber security in state government.

Introduction

Purpose

The Protecting Personal Information– the Privacy Fundamentals (the Fundamentals) has been developed to assist agencies in managing personal information and protecting individual privacy. It aims to provide practical guidance and best practice privacy measures to ensure the personal information your agency handles, is respected and proactively managed.

Importantly, the Fundamentals underpin the Information Privacy Strategy.

The Fundamentals focuses on information privacy. Information privacy can be defined as a person's entitlement to exercise control over their own personal information, in balance with the broader public interest.

Compliance

South Australian government agencies are required to comply with the Department of the Premier and Cabinet (DPC) Circular PC012 - Information Privacy Principles Instruction (IPPI).

Under the IPPI, the Principal Officer[1] of each agency is required to ensure the IPPI is implemented, maintained and observed in respect to the personal information the agency collects and uses in undertaking their role within government.

Under the IPPI, an agency means a public sector agency as defined in Section 3(1) of the *Public Sector Act 2009*.

Implementation

The Fundamentals does not need to be read in any particular order however it does provide a systematic approach to managing personal information.

You can choose to focus on particular areas needing improvement or areas identified as particular risks.

The Fundamentals may be used by any staff who work with personal information to undertake services, or those responsible for protecting information privacy in the agency.

In addition, the Fundamentals can be used more broadly to support local government and universities as a best practice approach to information privacy.

Other resources relevant to the Fundamentals include:

» Information Privacy Strategy

[1] "principal officer" means in relation to an agency: (a) the person holding, or performing duties of, the Office of Chief Executive Officer of the agency; (b) if the Commissioner for Public Employment declares an office to be the principal office in respect of the agency - the person holding, or performing the duties of, that office; or (c) in any other case - the person who constitutes that agency or, if the agency is constituted by two or more persons, the person who is entitled to preside at any meeting of the agency at which the person is present.

- Information Management Standard
- Information Governance Guideline
- South Australian Protective Security Framework
- South Australian Cyber Security Framework
- Open Data Framework.

Personal information privacy – the basics

What is personal information?

Personal information is defined in the IPPI as ‘information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from that information or opinion’.[2]

While a natural person is taken to be a living person there may be different considerations for information about the deceased. Agencies are encouraged to respect the sensitivities of family members when using or disclosing such information.

Agencies are also encouraged to respect the sensitivities of family members when using or disclosing personal information pertaining to First Nations people.

Personal information can include combinations of:

Name	Address	Phone number
Email address	Date of birth	Signature
Financial or health status	Witness statements	Photographs
Gender	Ethnicity	Religion
Alleged behaviours and licensing details	Biometrics (fingerprints, retina scans, gait)	Video footage

The important question to ask in determining whether information is personal is whether it can identify a particular individual.

Personal information can be collected in a variety of ways, for example in paper form, verbally or electronically.

Why is information privacy important?

Information privacy is important because people care about how their personal information is handled.

The South Australian government relies on information supplied by individuals for implementing and managing public services. This information often includes

[2] Information Privacy Principles Instruction

identifying details and is provided with a level of trust in how the information will be handled.

If an agency can be open and transparent about how and why they collect, use, disclose and store personal information, people are more likely to engage with them and trust that government places value in the personal information it holds.

Conversely, people can quickly lose trust in agencies that don’t treat their information properly.

There can be negative consequences and potential harm to an individual if personal information is not handled appropriately. Harm can occur in a variety of ways with lost, stolen or misused personal information: emotional distress, financial risk, intimidation, physical harm, discrimination, to name a few. What might be considered a minor amount of harm to one individual, may be significant to another.

Failing to respect the right to personal information privacy can have broader impacts too. Broken trust can lead to individuals withholding or falsifying information which can lead to failure of programs, projects, operations and outcomes that agencies seek to achieve.

Personal Information Privacy Management Framework

The Information Privacy Strategy recognises the need for a personal information privacy management framework (the Framework) that reflects best practice and provides a principles-based approach to proactively protect an individual's information privacy.

It is built around the following high-level elements:

- **Respect**. Keeping the interests of the individual front of mind by taking action to incorporate and improve the protection of individual information privacy.
- **Information Safety and Security**. All personal information is used, collected, stored, shared and disposed of safely and securely.
- **Data Minimisation**. Only collect the personal information required and only keep that information for the minimum amount of time.
- **Design**. Establishing methods and measures for protecting personal information privacy that are built into systems and practices, resulting in individual privacy being essential without compromising on functionality or business need.
- **Transparency**. Being upfront and open in the way personal information is managed, fostering trust in government's ability to protect individual privacy.

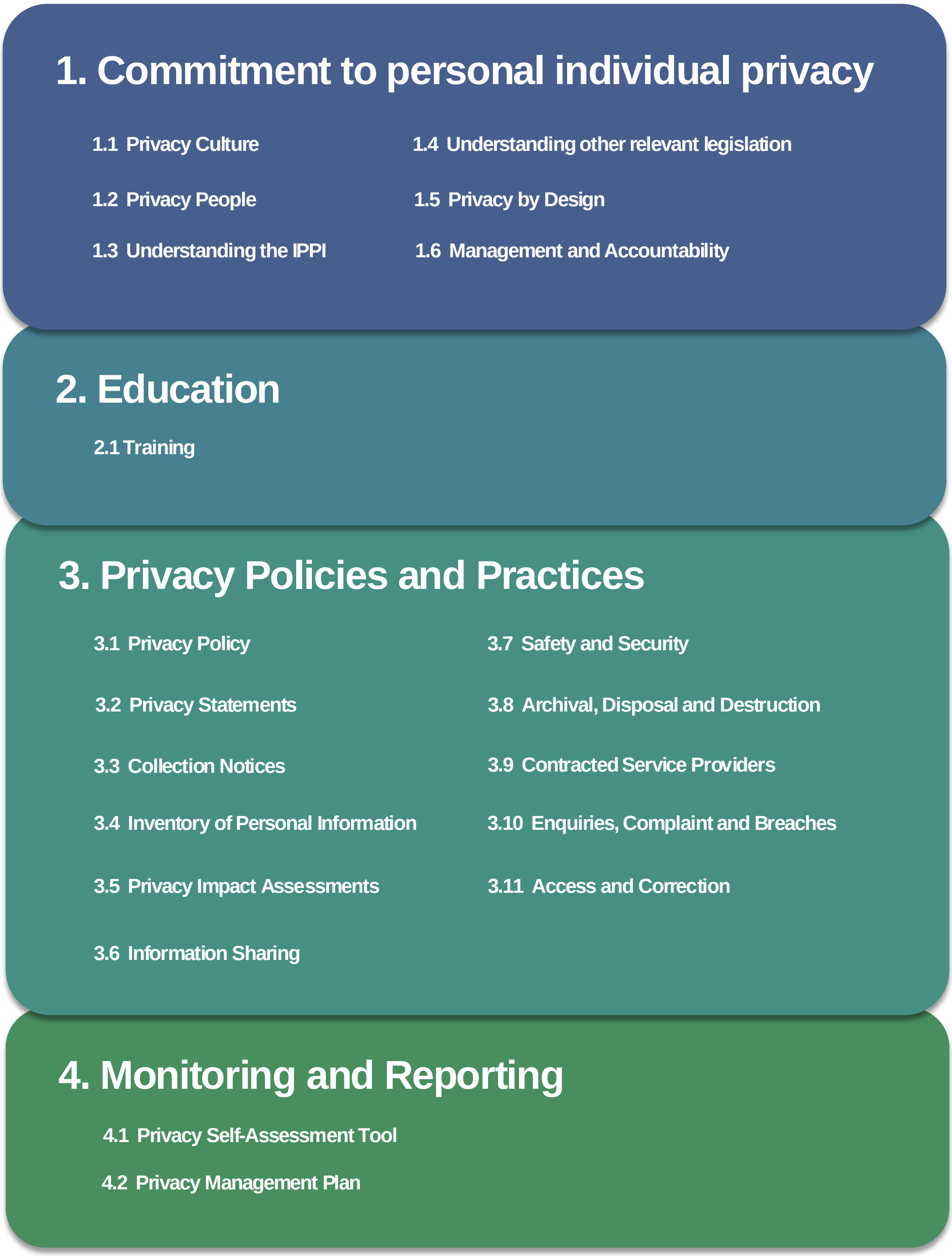
The Fundamentals steps through how to build a Framework to ensure personal information is managed appropriately.

The Framework can be separated into four parts:

1. **Commitment to Personal Information Privacy** – good information privacy governance and leadership foster a culture that respects privacy and prioritises individuals.
2. **Education** – staff are appropriately trained and know their information privacy obligations.
3. **Privacy Policies and Practices** – strong processes and policies manage privacy obligations and ensure compliance with the IPPI and privacy best practice.
4. **Monitoring and Reporting** – continuous improvement to ensure personal information privacy considerations remain current and are effective.

Collectively, these parts will help to develop a clear strategic direction for management of personal information privacy, as well as foster a good culture with a view towards continuous improvement.

Personal Information Privacy Management Framework



1. Commitment to personal individual privacy

- 1.1 Privacy Culture
- 1.2 Privacy People
- 1.3 Understanding the IPPI
- 1.4 Understanding other relevant legislation
- 1.5 Privacy by Design
- 1.6 Management and Accountability

2. Education

- 2.1 Training

3. Privacy Policies and Practices

- 3.1 Privacy Policy
- 3.2 Privacy Statements
- 3.3 Collection Notices
- 3.4 Inventory of Personal Information
- 3.5 Privacy Impact Assessments
- 3.6 Information Sharing
- 3.7 Safety and Security
- 3.8 Archival, Disposal and Destruction
- 3.9 Contracted Service Providers
- 3.10 Enquiries, Complaint and Breaches
- 3.11 Access and Correction

4. Monitoring and Reporting

- 4.1 Privacy Self-Assessment Tool
- 4.2 Privacy Management Plan

1. Commitment to personal information privacy

1. Commitment to personal information privacy

2. Education

3. Privacy Policies and Practices

4. Monitoring and Reporting

Information privacy should be intentionally integrated into your agency’s processes and procedures and day-to-day activities.

When protecting information privacy and personal information, the interests of the individual need to be kept front of mind.

Ideally, all staff and contractors should have an awareness of individual information privacy and an understanding of how the agency manages personal information, and why.

The agency’s culture should support the notion that personal information is managed in line with privacy best practice, with a clear commitment to do this.

A commitment to information privacy can be achieved by:

- leadership promoting a privacy culture
- staff awareness and understanding of the IPPI
- having dedicated staff, that are aware of the agency’s information privacy obligations, as well as privacy best practice
- understanding other legislation relevant to your agency that impacts personal information and information privacy
- applying privacy by design approaches, and
- integrating management and accountability of privacy measures.

1.1. Privacy Culture

A good starting point is management showing leadership in building a privacy culture and promoting good information privacy governance. In doing so, it shows staff that privacy obligations are taken seriously.

At the same time, it demonstrates to the public that the protection of personal information and information privacy are fundamentally important aspects of the public services offered.

There is no right or wrong way to build an information privacy culture but options can include:

- publishing privacy information on the intranet or website including readily accessible information, tools and resources on the collection, use, disclosure and storage of personal information.
- regular in-house information privacy updates, emails or bulletins. Keeping staff up to date and aware of any information privacy considerations.
- incorporating privacy measures into agency documentation, for example strategic plans. Having privacy included in templates and documentation ensures the protection of personal information privacy is integrated into organisational processes.
- incorporating the protection of personal information privacy into staff training:
  - agency induction – new staff are introduced to the information privacy culture at the commencement of their employment and made aware of the privacy measures that are in place to handle personal information.
  - information sessions – training for all staff focussing on protecting personal information, the importance of respecting individual information privacy and the risks associated with not managing personal information correctly.
  - targeted workshops – this may be more important for particular teams and / or business units dealing with personal information for example project managers, Information and Communications Technology (ICT), enquiries and complaints, Freedom of Information (FOI).
- a section / team dedicated to the management of information privacy obligations. This section could support agency staff with information privacy advice, assessment of projects and associated privacy risks, enquiries, complaints and breaches. It could include ICT, risk, legal, records management and information management to provide a comprehensive approach to protecting personal information privacy.

1.2. Privacy People

It is a good idea to have agency staff dedicated to the protection of personal information privacy and to manage day-to-day information privacy requirements. Staff who have knowledge of internal privacy matters can ensure compliance with the IPPI and that personal information is appropriately collected, used, disclosed and stored.

Dedicated privacy officers can:

- create privacy awareness and contribute to fostering a privacy culture
- develop and implement agency-specific information privacy policies

- provide internal advice regarding information privacy obligations when dealing with personal information
- assist with privacy impact assessments that need to be undertaken for projects involving the collection and handling of personal information. This could include the coordination of different teams that need to be involved with the project to assess and minimise privacy risks
- network with other key staff in FOI, records management, ICT, security, and project and service development
- respond to any queries, complaints and breaches, as well as requests for access to personal information
- consider information sharing needs and requests from other agencies
- provide assistance and guidance prior to engaging with contracted services providers to ensure contracts include IPPI obligations. This can include contracts such as consultancies for policies or projects, external information assets storage or confidential destruction of information assets
- ensure continuous improvement by taking lessons learnt and revising and reviewing the policies and procedures relating to personal information and information privacy.

Contact channels for privacy staff should be published, providing a direct communication avenue for the public for privacy enquiries and complaints or for any other information privacy related matters. It also demonstrates transparency in the processes in place to manage individual privacy matters.

1.3. Understanding the Information Privacy Principles Instruction

It is necessary to understand the requirements of the IPPI – the principles and other considerations for appropriately managing personal information.

The IPPI exists to ensure personal information collected, used, disclosed and stored by state government agencies is managed appropriately. The Principal Officer of each agency must ensure that the principles in the IPPI are implemented, maintained and observed.

Please note:

If your agency has a legislated requirement to collect, store, use or disclose personal information, then that legislation takes precedence.

The 10 principles ensure that:

- » information is collected with the individual’s awareness and permission
- » information is used and disclosed appropriately
- » information is kept safe and secure – whether hard copy or electronic
- » individuals can access the personal information an agency holds about them, and

- individuals can get their personal information corrected if it is not up to date or accurate.

The principles recognise the need to balance personal information privacy with the broader public interest.

Each agency should have policies concerning the storage and classification of personal information in accordance with the requirements of the South Australian Protective Security Framework[3] (Premier and Cabinet Circular 30), the South Australian Cyber Security Framework[4] and information management standards and guidelines.

If you are unclear about your agency's security policies or procedures you should contact your Agency Security Advisor and/or Information Technology Security Advisor.

Personal information should only be used for the purpose it is collected and it should not be used for another purpose or disclosed to a third person. There are several exceptions outlined in the IPPI:

- if the record-subject would reasonably expect the information to be used or disclosed for a secondary purpose (which must be related to the primary purpose)
- the record-subject has consented to the use or disclosure
- the use or disclosure may prevent or lessen a serious threat to life
- the use or disclosure is required by law
- the use or disclosure is for the enforcement of law
- the agency suspects unlawful activity and the use or disclosure can assist with an investigation or for reporting to relevant authorities, or
- the use or disclosure relates to a person who has engaged or may engage in illegal conduct or serious misconduct regarding a person and complies with any guidelines issued by the Minister.

Example:

The police are aware that a male with a history of child sexual assault convictions has begun to cohabitate with a single mother of two girls, aged 8 and 12. The mother may or may not be aware of the male's history. She may or may not be leaving her children in the unsupervised care of the male. It is reasonable for the police to believe that it is necessary to disclose this information to the mother to prevent a serious threat to the health and safety of the children.

[3] The South Australian Protective Security Framework describes the arrangements and expectations for personnel, physical and information security in South Australian government agencies.

[4] The South Australian Cyber Security Framework (SACSF) is the whole of South Australian government cyber security policy framework. The SACSF directs and guides agencies through an approach for establishing, implementing, maintaining and continually improving their cyber security posture.

1.4. Legislation

In South Australia, no specific state privacy legislation exists. However, there are other South Australian laws that protect elements of information privacy, including (but not limited to):

- Public sector employees are bound by the Code of Ethics issued under the *Public Sector Act 2009*, which requires public sector employees to "…ensure that the privacy of individuals is maintained and will only release information in accordance with relevant legislation, industrial instruments, policy or lawful and reasonable direction."
- *Freedom of Information Act 1991* – functions to protect the personal affairs of individuals when providing access to information. Additionally, it provides a mechanism for the public to apply to amend their personal information.
- *Criminal Law Consolidation Act 1935* – actions that are illegal and criminally liable under South Australian law, including section 144C regarding the misuse of personal identification information.
- *Public Sector (Data Sharing) Act 2016* – enables public sector agencies to share data with each other and with some external entities. It promotes the management and use of public sector data as a public resource that supports good government policy making, program management and service planning and delivery.
- *Surveillance Devices Act 2016* – regulates the use of surveillance devices and protects against the installation of devices to record or observe a person, place or activity without authorisation. The Act predominantly applies to private activities and conversations and does not typically apply to activities that occur in public places.
- *Summary Offences Act 1953* – makes provision for certain offences against public order and for a broad range of other summary offences. It is relevant for crimes that impact on an individual's privacy.
- *Education and Children's Service Act 2019* – provides for preschool, primary and secondary education in South Australia. Section 14 deals with information sharing and section 137 deals with confidentiality.
- *Children and Young People (Safety) Act 2017* – protects children and young people from harm noting that mandatory notifications will require the disclosure of personal information (see Chapter 5). Section 152 deals with information sharing and section 164 deals with confidentiality.
- *South Australian Public Health Act 2011* – promotes and provides for the protection of the health of the public for South Australia. Sections 99 and 100 deal with confidentiality.
- *Health Care Act 2008* – provides for the administration of hospitals and other health services. Section 93 deals with confidentiality.

- *Mental Health Care Act 2009* – provides for the treatment, care and rehabilitation of persons with mental illness and provides protections of the freedom and legal rights of persons with mental illness. Section106 deals with confidentiality and disclosure of information.

It is important to be aware of agency specific legislation which governs the management and sharing of personal information.

What about the Commonwealth *Privacy Act 1988*?

The *Privacy Act 1988* (Commonwealth) applies to Commonwealth government agencies, private companies and private health providers, with some exceptions. It **does not** apply to:

- private companies with a turnover of less than $3 million unless they are handling health information or trading in personal information
- state government agencies (with exceptions)[5]
- local government authorities and
- private companies that are contracted service providers of state government agencies, in respect of work they are undertaking for or on behalf of a state government agency.

The Commonwealth Act is administered by the Office of the Australian Information Commissioner.

General Data Protection Regulation

The European Union (EU) General Data Protection Regulation brings consistency to data privacy across the EU as well as providing improved privacy protections for individuals. This Regulation impacts agencies providing services to EU citizens.

State Records has developed an information sheet that provides more details relating to the Regulation.

1.5. Privacy by Design

Privacy by Design (PbD) is an approach that incorporates good privacy practices into decision making.

It ensures proactive privacy consideration in the design, development and implementation of any program or initiative that collects, uses, discloses or stores personal information.

Basically, the protection of an individual's information privacy is integrated into all agency aspects. Information privacy is considered early and often, which allows for potential risks to be identified and addressed.

PbD offers the following benefits:

[5] The Notifiable Data Breach Scheme applies to South Australian government agencies if the breach includes Tax File Numbers.

- it builds information privacy awareness and an understanding of how to handle personal information
- it builds public trust as your agency demonstrates the value of the personal information it holds
- it encourages prevention rather than compliance as information privacy is considered early and integrated into operations
- it reduces information privacy risks, as risks are identified early and measures are implemented to mitigate those risks, and
- it has the potential to reduce any remediation costs.

Implementation of PbD can vary depending on the size of the agency, the systems used, the types of projects undertaken and the amount and sensitivity of personal information collected.

Approaches that can be taken to implement PbD include:

- the promotion and championing by executive and senior management of good information privacy practices (Section 1.1)
- consulting with dedicated privacy staff on all programs or initiatives that involve personal information (Sections 1.2)
- having current, clear and accessible information privacy policies that explain how your agency manages the personal information it collects, uses and holds, as well as promoting transparency to build public trust (Section 3.1)
- only collecting and using the information needed
- providing detailed, easy to understand collection notices when collecting personal information (Section 3.3)
- publishing roles and contact channels for the staff who manage privacy in the agency (Section 1.2)
- using and storing personal information with the minimum amount of detail, de-identified or grouped together, so it's protected but still usable for the purpose it was collected (Section 3.7)

Example:

Agency ABC offers a range of online services. After a customer uses an online service, a survey pops up seeking feedback and suggested improvements of the service.

The survey does not ask for the details of the customer (e.g. name, email address). This information is not needed and therefore not collected.

Example:

Agency DEF engages a consultant to review several systems to improve customer services.

The work includes a review of several different systems as data on individuals spans several systems. The data on an individual is securely extracted from each system, given a coded identifier and then identifying names and contact details are removed.

Only the de-identified information is needed and used for the review.

- adopting a ‘plain language’ policy for any public documents (Sections 3.1-3.3)
- at the commencement of any new project or initiative, completing a privacy impact assessment (Section 3.5)
- implementing appropriate security measures throughout a project’s lifecycle to protect personal information (Section 3.7), and
- having clear processes for destroying or de-identifying personal information as soon as it is no longer needed (Section 3.8), subject to disposal obligations under the *State Records Act 1997*.

Implementation of any of these measures is a step towards creating and building a commitment to protecting information privacy and a privacy culture where it is evident that the personal information held is respected and managed appropriately.

Case Study – How Privacy by design can be of benefit

In this case study, we will look at two agencies, one with privacy by design features embedded in the organisation and one without and see how the implementation of a new initiative required by management is navigated.

Scenario

The agency is looking at cost saving measures and efficiencies and has decided to outsource storage of information offsite in the cloud. The project budget is $400k to secure a provider.

The information (digital information assets) to be stored offsite includes customer information of closed cases. The information assets record the following personal information:

- Name
- Address
- Telephone number
- Date of birth
- Driver's licence number
- Case notes and decisions

The information has been sentenced and needs to be retained temporarily for 50 years

Agency Red

Agency Red has not considered the importance of individual privacy or prioritised privacy within the organisation. No steps have been taken to implement privacy measures in the organisation.

The assigned Project Manager (Jamie) sets about developing a project plan. The plan focuses on staff required for the project, relevant approvals, costs and timeframes.

Jamie recognises the ICT team will need to be involved and procurement will help with the process of engaging a service provider.

The ICT team advise Jamie of the South Australian government policy that a risk assessment is required for any outsourced or offshore ICT information requirements.

The risk assessment is undertaken, with appropriate focus on robust ICT platforms, technological compatibility and value for money.

Jamie considers the risks involved with the project can be appropriately managed.

Agency Green

Agency Green understands how important individual privacy is and has incorporated many privacy measures throughout the organisation to address individual privacy and associated risks. Personal information is respected and managed appropriately.

The assigned Project Manager (Jesse) sets about developing a project plan. Jesse has previously undergone privacy training and understands such an initiative may include some risks to the agency. Jesse knows a privacy impact assessment (PIA) is necessary to establish what personal information will be involved in the project and if there are any risks to the agency.

As the agency actively promotes privacy, Jesse knows there are resources available on the intranet to assist, for example a PIA template.

Jesse also recognises other areas of the agency will need to be involved and contacts the dedicated privacy team, the ICT team, procurement, legal and information management teams for input and assistance.

A PIA is undertaken during the planning stage of the project with all relevant stakeholders. Several questions are raised:

- Will the personal information be sent outside of South Australia or Australia, and if so, is there any breach of local law?
- Does the service provider comply with legislation/standards of South Australia?
- Is the personal information subject to the legislation of the storage jurisdiction? Will the service provider keep the personal information safe? Can the agency access their information assets under their legislation?
- Will the information be stored overseas? Are there sufficient protections in place to manage this?
- Is there a risk of unauthorised access?
- Can the agency still access the information assets for its own business or legislative (FOI) requirements?
- Can disposal of the information assets occur in line with the State Records Act? Will the information assets be returned to the agency?

Jesse understands the contractual obligations placed on the service provider will help to mitigate most of the risks identified.

Scenario

The project is put out to tender with three providers showing interest in the job:

Blue Box Records – $500k – has similar protections to Australian privacy law but refuses to consider and include the Information Privacy Principles Instruction (IPPI) as part of the terms and conditions of the contract.

Records Are Us – $350k – has basic protection of information measures included in the terms and conditions of the contract.

Record Keepers Inc - $600k – has robust protection measures in place for managing personal information securely and will include the IPPI as part of the terms and conditions of the contract.

Agency Red

Agency Red does a little due diligence to discover all of the providers have at least a basic level of protections in place for information storage.

It decides to go with **Records Are Us**, as the project will come in under budget.

The contract ensures ownership remains with the agency and there is access to the information assets when required. It does not include privacy provisions, nor mention the IPPI.

Agency Green

Agency Green has concerns that **Blue Box Records** and **Records Are Us** don't adequately protect the stored information and don't comply with the IPPI. In addition, they subcontract parts of their operations increasing risks, whereas Record Keepers Inc do not.

It is decided **Record Keepers Inc** is the preferred provider but recognising the cost ($200k over budget), Jesse seeks senior management approval to proceed. Approval is granted.

Jesse, with the help of the dedicated privacy team, the ICT team, procurement, legal and information management teams, develops a contract with terms and conditions focussing on the safety and security of the personal information. Whilst the information will be stored in a different state, the contract ensures the jurisdictional legislation relating to the information assets where stored doesn't apply and instead the provider complies with the IPPI. In addition, there is a process in place to access the information assets.

Scenario

The contracts are finalised and the go live date is set for 30 November. During the transition period in November, several industry providers experience a cyberattack resulting in some data being stolen.

Agency Red

Unfortunately, Agency Red was affected by the cyberattack.

Part of **Records Are Us** business process was to subcontract parts of their operation to **Rose Repositories** (with little regard for privacy) and the transfer process resulted in the inadequate protection of the agency's personal information. 400 individuals were affected.

Jamie and Agency Red didn't know what to do about the breach or how to manage it. By the time they understood it was necessary to advise the affected individuals, some of those individuals had already suffered harm. This resulted in some significant costs for the agency, damaged reputation and trust in government, including extensive media coverage.

Agency Green

Fortunately, Agency Green contracted with **Record Keepers Inc**, with privacy measures and the safety and security of personal information included and implemented as part of the contract (the IPPI was included in the terms and conditions, along with rigorous security requirements). In practice this meant, the agency information was kept safe and was secured to a high standard and was resistant to the cyberattack.

Had a breach occurred, Agency Green was well prepared to manage it with an agency breach response plan part of business process.

Conclusion

Agency Green

Agency Green was well placed to manage the project as privacy measures already implemented in the agency demonstrated a streamlined approach to implementing the new initiative.

All staff understood the importance of privacy and the correct management of personal information and the steps involved to achieve this.

Personal information was respected, protected and managed appropriately throughout the process.

Agency Red

Agency Red did not comprehend what would happen if personal information privacy wasn't considered in the project.

As a result, the agency encountered damaging and costly mistakes as well as a loss of stakeholder's trust, that could have been avoided.

1.6. Management and Accountability

With the right management and accountability measures in place, the responsibility for information privacy management should be clear to staff and the public.

In practice, this means roles and accountabilities for protecting personal information privacy are resourced, assigned, documented and well understood, and messaging regarding roles and accountabilities is tied to broader strategic objectives.

Performance in relation to information privacy management (for example, timeliness and quality), is measured and reported to senior management and learnings are implemented for continuous improvement. This may also include monitoring and addressing staff adherence.

2. Education

1. Commitment to personal information privacy
2. Education
3. Privacy Policies and Practices
4. Monitoring and Reporting

Education and training are critical to fostering a good information privacy culture and is further evidence of a commitment to good personal information management.

Appropriately trained staff will be aware of the benefits and obligations in valuing and respecting personal information and managing it effectively.

A vital part in education of staff is the support from leadership.

2.1. Training

Training is one way to educate staff about the importance of the appropriate collection and management of personal information and information privacy.

Before developing education and training tools, it is worth considering what message needs to be conveyed, as this may differ depending on the audience. For example, the message to:

- executive and senior management might emphasise that protecting information privacy supports achievement of business goals and objectives, whilst mitigating risk, as well as offsetting costs due to preventing privacy issues from occurring
- information technology professionals might focus on system reliability, safety and security to protect the personal information held
- teams working on program management, development or procurement, might focus on responsibilities for assessment of the privacy impact in overseeing the implementation of personal information management practices, and
- operational staff might focus on individual and collective responsibility to manage the protection of information privacy.

Training can be tailored not only according to the audience, but also for the competence of that audience, as some may be more involved with personal information than others. The frequency of messaging might also be different for each, affecting the style and content of the training.

Agency induction courses or training need to demonstrate how the agency manages personal information and information privacy. New staff should get an immediate sense that personal information is respected and is treated accordingly.

Ideally, all staff are made aware of any information privacy policies and processes (for example a privacy complaints process), where to access them and how to apply them.

The following table summarises options for different types of training and the means of delivery.

Training	Audience	Delivery Mechanism Options
Induction	New staff, contractors and volunteers	» Induction Package » Workshops » Online training modules
General awareness	All staff, including management, contractors and volunteers	» Key messages according to audience on the agency's policies and procedures relating to personal information and privacy » Workshops, one-on-one meetings or targeted sessions – overview of managing personal information and privacy within the agency » Online training modules » Website content and resources, easy to find and access » Regular updates
Tailored	Staff who specifically deal with personal information the agency collects, uses, discloses and stores	» Workshops, one-on-one meetings or targeted sessions regarding managing personal information and privacy » Online training modules » Website content and resources, easy to find and access

It is recommended that any privacy training available is reviewed and updated, including the provision of refresher training on a regular basis. This will ensure staff knowledge and skills are kept up to date or developed as information privacy management responsibilities change.

UNDER DEVELOPMENT

State Records Online Training Modules

State Records is developing the following training modules designed to assist agencies:

- Handling Personal Information
- How to conduct a Privacy Impact Assessment
- An overview of the Information Privacy Principles Instruction.

3. Privacy policies and practices

1. Commitment to personal information privacy

2. Education

3. Privacy Policies and Practices

4. Monitoring and Reporting

Policies, processes and practices around the collection, use, disclosure and storage of personal information should be developed and implemented.

The size of each agency and the amount of personal information managed may impact how many policies and procedures are required. A small agency might opt to integrate information privacy elements into other policies, for example records management or information management policies. A large agency with distinct functions and services may have multiple information privacy policies that each focus on the management of personal information within different business units.

At a minimum there should be:

- an information privacy policy
- a published information privacy statement
- collection notices at any collection points
- a register of the types and purposes of personal information held
- a privacy impact assessment process
- policies to support information sharing
- policies to support the safety and security of personal information
- a process for engaging with contracted service providers
- policies to support archiving, disposal and destruction of personal information
- a process for enquiries and complaints, and
- a process for managing and reporting privacy breaches.

3.1. Information Privacy Policy

An information privacy policy is a reference for staff to understand the processes and practices used to collect, use, disclose and store personal information. It also outlines to the public the agency’s processes.

To ensure it is effective, it should be clear, in plain language and transparent. It needs to provide enough information for individuals to understand how their personal information will be handled.

Every agency’s information privacy policy will be different to reflect the size and nature of the organisation as well as the different types of personal information it uses and holds.

An information privacy policy needs to explain how the personal information is collected and how that information flows through the agency. For example, the collection can be via hard copies, on the telephone or through online applications and websites.

The policies, processes and practices developed to manage personal information will form the basis of your agency’s information privacy policy.

An information privacy policy should include:

- the date of the policy
- the agency’s name
- the agency’s main functions
- the types of personal information collected and used
- how (and if) the personal information is shared
- how the personal information is stored and for what period of time, and
- the process for handling a privacy complaint and / or reporting a breach of personal information.

The information privacy policy needs to be kept up to date and should be published and easily accessible.

3.2. Information Privacy Statement

The aim of an information privacy statement is to help an individual understand how their personal information will be handled and as a result of the content of the statement, help them to decide if they will transact with the service. It needs to be concise, relevant, clear and accessible.

It differs from an information privacy policy as it is generally used at the point of a transaction with an individual, whereas an information privacy policy is a more comprehensive document that outlines the broader processes and procedures for handling personal information.

An information privacy statement can explain how personal information is collected via websites, mobile applications and social media services. Information may be collected overtly, such as when an individual is asked to provide information directly or collected covertly through a web server or cookies.

It is important that users also understand what will happen to their information after collection, allowing them to make an informed decision before proceeding.

Information in an information privacy statement should include:

- what personal information is collected and for what purpose
- if it is authorised or required by or under law

- how the personal information will be used
- if it will be disclosed, to whom, and why
- how an individual can access or correct their information
- any automatic or covert collection of information through cookies or clickstream data, and
- any other relevant privacy issues.

An information privacy statement should link back to the information privacy policy.

3.3. Collection Notices

Whilst an information privacy policy provides a general overview of how personal information is handled and an information privacy statement is used at the point of a transaction with an individual, a collection notice informs an individual of your agency's intention of collecting personal information and what it plans to use it for.

A collection notice might be printed on a form or posted at a service point.

Importantly, a collection notice relates to a specific purpose. Agencies should only collect personal information that is required for the specific purpose and that information is used, stored, shared and disposed of safely and securely.

If there are multiple reasons (such as projects) to collect personal information each with a different purpose, then multiple collection notices might be required for each purpose for which personal information is collected.

If information is not required for an intended purpose, then don't collect it. There is no benefit to collecting excess information that needs to be appropriately managed if the agency has no use for it. To do so only increases the risks to the agency.

Example:

Agency MNO wants to keep track of the number of visitors to their website, including which site the referral came from. The agency keeps count of visits and records the referring site but does not keep IP addresses of visitors as this information is not necessary.

Clear collection notices promote transparency and allow an individual to provide informed consent prior to the collection of their personal information.

For reference, principles 1-3 in the IPPI set out the requirements around the collection of personal information.

A collection notice should include:

- the collecting agency
- the reasons for collection and the authority for collection
- what the personal information will be used for and if it will be disclosed to any other parties

- how an individual can apply to access or amend their information
- how long the information will be kept
- that the information will be kept secure
- how a complaint can be made, and
- the main consequences (if any) if all or part of the information is not provided.

Example:

To streamline customer service, Agency JKL has set up an online verification system that uses voice prompts for users to log in. A customer can opt not to use this system to log in and is advised of an alternative process to phone to log in and access their account.

3.4. Register of Personal Information

To assist with information privacy governance – and governance of all information assets – it can be useful to keep a register of personal information.

Having such a register ensures there is awareness of the personal information handled, where it is kept (including third parties) and the risks associated with known practices around collecting, using, disclosing and storing that information.

The register does not need to include any personal information within it, but should include:

- the type of personal information
- whether the information constitutes sensitive information
- the purpose for which the information was collected
- the legal authority under which the information was collected
- how and where the personal information is stored (including whether it is stored overseas, with a cloud service provider, or other third party)
- who is authorised to access the information
- how long the information will be retained, and when and how information will be de-identified or destroyed.

Maintaining a register of the personal information holdings will assist with:

- understanding how the personal information collected can be used and disclosed
- ensuring the personal information is safe and secure
- easily responding to requests to access or correct personal information
- keeping the information privacy procedures and systems up to date and relevant, and
- assessing any inherent risks involved in the personal information that is held and the way it is handled.

In practice, the content of the register of personal information should be developed collaboratively by the various teams responsible for the management of personal information. Any existing procedures around security classification of information assets may help to identify the personal information held.

Personal information elements can be added into an agency-wide information asset register (see also the requirement for an information asset register in the Information Management Standard and Information Governance Guideline).

The register should be regularly reviewed and updated to ensure that it reflects the current personal information held.

3.5. Privacy Impact Assessment (PIA)

A PIA is a tool used to identify, assess and minimise privacy risks when managing personal information in relation to specific projects, programs or systems.

A PIA is an important step in support of PbD.

Undertaking a PIA is particularly useful when embarking on a new project or initiative or amending an existing one, even if it is not yet known whether there will be a privacy impact.

A PIA will likely uncover any privacy risks at an early stage in the process allowing correction before the risk can occur.

It also builds compliance with the IPPI into the project.

When considering whether to undertake a PIA, every project should be assessed individually. If you have multiple projects that each collect and use personal information differently, then a PIA should be undertaken for each project.

A PIA involves an assessment of a project or initiatives:

- positive and adverse privacy impacts
- compliance with the IPPI and other relevant legislation, and
- controls that mitigate any identified risks.

After completing a PIA, you will have a comprehensive assessment of how the agency will handle the personal information required for the project, how any privacy risks will be managed and whether the project can proceed or not, based on those assessments.

Example:

Agency PQR has conducted a PIA in the planning phase of a new project, gathering details on what personal information is required for the project, how that information will be collected, who will need access to the information once collected and how it will be safely stored for the project's duration.

The PIA has been signed off by senior management, allowing the required personal information to be collected for the project with the relevant approvals and risks addressed.

A PIA can be used as a reference for future actions of a project. It should be kept current and relevant to the project and should be adjusted if required throughout the life of the project.

To improve transparency, it is a good idea to make PIAs available on the agency's website, subject to redaction of any confidential information.

UNDER DEVELOPMENT

State Records is developing a PIA Guideline. The Guideline will assist with threshold assessments which will help determine whether a PIA is required and then will step through the PIA process. It will have templates to assist agencies.

In addition to the Guideline, State Records is developing an online training module 'How to conduct a Privacy Impact Assessment'. This training will provide an interactive case study stepping through how to under a PIA.

3.6. Information Sharing

Sharing of personal information across government is allowed in prescribed circumstances. Allowable disclosures include where the disclosure is authorised by law, for the enforcement of law or to prevent or lessen a serious threat to the life, health or safety of someone. Principle 10 of the IPPI sets out instances where disclosure is allowed.

Where an agency needs to share personal information, it should ensure appropriate controls are in place to keep the information safe.

To assist, the South Australian *Public Sector (Data Sharing) Act 2016* (PSDS Act) provides a framework to share information by state government agencies. The 'Trusted Access Principles' under section 7 of the PSDS Act specify requirements that must be satisfied to share data. These requirements are referred to as the 'Five Safes', which include safe projects, people, data, settings and outputs.

The Information Sharing Guidelines (ISG) are designed to give providers of services to children, young people and adults, confidence in sharing information when required to prevent harm or respond to current threats to safety and wellbeing.

DPC has two training modules designed to aid in the use of the ISG:

» Introduction to Information Sharing Guidelines for Promoting Safety and Wellbeing – a 15-minute overview of the ISG.

» Information Sharing Guidelines for Promoting Safety and Wellbeing Induction for Staff and Supervisors – a 45-minute course targeted to front line staff, supervisors and policy makers who have detailed knowledge of the ISG and its application in their work.

You can find these training courses on DPC's website.

The IPPI operates alongside the ISG and **does not** provide a barrier to the collection, use and disclosure of information necessary to promote the protection of children and young people.

If a state government agency intends to undertake a program or action of significant public interest that does not comply with one or more of the principles within the IPPI it may apply to the Privacy Committee of South Australia for an exemption. Exemptions are published in the Privacy Committee's Annual Report.

3.7. Safety and Security of Personal Information

Keeping personal information safe and secure is extremely important as it reduces the risk of harm to individuals caused by breaches and reduces any risk to unauthorised use, misuse, loss or theft.

The safety of personal information closely aligns with good information management practices. If information is managed well by the agency, there is a good chance personal information is already being safely protected.

State Records provides guidance on information management:

- Information Management Strategy which provides the principles to be followed by agencies to ensure information assets (which includes personal information) can be relied on and are trusted.
- Information Management Standard which outlines expected behaviours required to effectively manage information assets, achieve business objectives and meet legislative and policy obligations.
- Information Governance Guideline which supports agencies in meeting their information keeping requirements under the *State Records Act 1997* via the Information Management Standard, and
- Managing Digital Records in Systems Standard which ensures all business systems and records management systems maintain the integrity and reliability of the digital information stored in them.

It is also prudent to have appropriate safeguards in place when engaging with third party providers, including model contract terms to cover compliance with the IPPI and the *State Records Act 1997*. These safeguards will ensure your agency will keep any personal information safe when engaging with third party providers. Refer to section 3.9 for further detail on contracted service providers.

Information security considers the protection of information throughout its entire lifecycle: from when information is collected, while it is held by the agency and when it is disposed of.

The South Australian Protective Security Framework (SAPSF) provides state government agencies with policy requirements and guidance to implement and maintain effective security measures and manage security risks.

Your agency can design security policies and procedures in a way that supports the IPPI.

Strong guidance and training about information security promotes a security culture. It also helps individuals understand the importance of good information handling practices.

Assigning classifications (for example sensitive or classified information) to information, including personal information, can ensure appropriate management of that information. The higher the classification, the more important or sensitive the information and the more enhanced security measures needed to keep it secure.

Access permissions and restrictions can also secure personal information. If only a handful of people need access to the personal information, restrict access from everyone else to keep the information safe and secure. Logging or recording access to personal information is also important to detect and investigate breaches.

Personal information, both hardcopy and electronic, can be kept secure by having appropriate storage facilities. This can include onsite compactus, with relevant / restricted access, electronic records management systems with appropriate classification and access levels and server rooms with appropriate access authorisation protections. It can also include having ICT systems and equipment that is appropriately protected.

Security measures include having appropriate authorities and controls for the collection and management of personal information, as well as the necessary physical or digital access and security classifications. In addition to managing authorised access, security controls ensure that the information remains authentic and reliable as evidence of decisions and actions taken. This means it must be capable of being retrieved in a readable format later.

Measures such as clean desk policies, computer log ins and building security can all contribute to keeping personal information safe and secure.

It is also important your agency has a process in place to manage a security breach. This should include response timeframes, who manages the breach, actions taken and who receives the breach notification. Refer to section 3.10 for further detail on managing breaches.

3.8. Archival, Disposal and Destruction of Personal Information

Processes should already be in place for archiving, disposal and destruction of information assets when no longer required. Holding personal information for longer than the authorised disposal term poses a possible risk to your agency.

Destruction or retention of personal information must be undertaken in accordance with a disposal determination (in the form of a disposal schedule) authorised under the *State Records Act 1997*. Disposal includes a range of processes associated with implementing information assets retention, destruction and transfer.

Example:

Due to financial constraints and competing priorities, for five years, Agency STU has not been able to undertake the authorised disposal of research reference material including medical information.

A cyber-attack resulted in the theft of this medical information and the breach impacted many individuals.

Had this information been disposed of at the appropriate time, the breach would not have occurred.

Personal information may be held within an electronic document records management system, business system or in physical files. Regardless of where personal information is held, the information assets must be managed in accordance with your agency's records management policies and procedures, and destruction can only occur in accordance with current approved disposal schedules.

In the first instance, seek advice from records management / information management team experts. State Records is also available for further advice.

3.9. Contracted Service Providers

It is common practice for government to engage private sector organisations to provide services on their behalf.

The IPPI recognises this practice and includes provisions to ensure both agencies and the contracted service providers are accountable for the protection of the personal information they handle.

The IPPI requires personal information handled by contracted service providers, undertaking a service on behalf of government, to be treated in the same way it would be if the agencies themselves were delivering the service.

The Contracting and Information Assets Standard issued under the *State Records Act 1997*, assists agencies to incorporate information management requirements into the contracting process.

The Contracting and Information Assets Guideline provides support and additional practical advice in relation to information management requirements when contracting with a service provider.

The Standard must be applied to all South Australian government contracts.

To assist agencies to meet their contractual obligations, model terms and conditions have been developed by the Crown Solicitor's Office.

The Standard, Guideline and model terms and conditions are all available on the State Records website.

The importance of good contract management practices should also be considered when contracting with service providers. In addition to the inclusion of privacy requirements in a contract, best practice would be to set key performance indicators against those requirements with active monitoring of the service provider's performance throughout the duration of the contract.

3.10. Enquiries, Complaints and Breaches

Processes to manage information privacy enquiries, complaints and breaches should include what to do, who to advise, who to contact and how to manage issues and / or breaches when they occur.

Advice should be easily found by members of the public wishing to progress a privacy enquiry, complaint or advise of a breach.

Existing feedback, complaints, compliments and threats processes can be adapted to include privacy enquiries, providing there are additional steps included to address complaints and breaches.

PC039 – Complaint Management in the South Australian Public Sector requires all South Australian public sector agencies to establish and maintain an effective complaint management system.

Enquiries

Having staff responsible for managing information privacy enquiries will help to apply their knowledge and familiarity of the agency's information privacy measures.

The published policy and process covering the handling of enquiries, should advise who manages the enquiry and the timeframes for responding. Advice about how privacy enquiries will be handled, by whom (i.e. which role) and in what timeframe, should be easily accessible to the public.

A published enquiry form provides a template with required information fields for users to populate, so the enquiry covers the detail needed. It can also ensure only the required personal information is provided. If your agency uses online forms, it will need to have the appropriate security measures in place to make sure any personal information obtained from a completed form is kept safe and secure.

The enquiry form should include its own collection notice and indicate whether the enquiry may need to be escalated to another area or agency for action.

Complaints

In the first instance, members of the public should make information privacy complaints directly to the agency or business unit, to be resolved through an existing complaints handling process.

As with enquiries, having a form and published process helps to achieve a successful outcome for all parties involved.

If a privacy complaint is unable to be resolved directly by your agency or the individual is dissatisfied with the response, the individual can choose to make a complaint to the Privacy Committee of South Australia. Contact details for the Committee are listed under Breaches.

More information about privacy complaints can be found on the State Records website.

The Privacy Committee of South Australia is established by Proclamation (set out in the IPPI) and reports to the Attorney-General. It exists to:

- Make recommendations to the government and any person or body on measures that should be taken to protect personal information.
- Oversee the implementation of the IPPI by South Australian public sector agencies.
- Refer written complaints received about breaches of information privacy to the relevant authority.

Breaches

A privacy breach occurs when personal information "that is not already publicly available, is lost or subjected to unauthorised access, use, modification, disclosure or misuse"[6].

[6] Personal information Breach Guideline

A breach may occur because of accidents, procedural errors, or deliberate actions, such as theft or unauthorised access.

The Personal Information Breach Guideline advises agencies how to be prepared for and respond to privacy breaches.

The steps involved in managing a breach include reporting the breach, identifying the risks, notifying the affected parties and implementing remedial action.

Each agency should have a breach response plan, with clear processes in place for when a breach occurs.

For privacy breaches by state government agencies, the Privacy Committee of South Australia must be notified. The Privacy Committee is responsible for oversight of the IPPI. They receive and review complaints and breaches of privacy to gain understanding of trends or risks across government and can offer advice on remedial actions.

There are other authorities that also need to be notified of a breach, depending on the circumstances:

- The SA Government Cyber Security Watch Desk – for breaches that involve digital information
- South Australia Police – for breaches that may be the result of criminal actions
- Office of the Australian Information Commissioner – for breaches that relate to tax file numbers.

State Records has developed a Privacy Breach Notification Template to notify the Privacy Committee.

For further assistance, the Privacy Committee's Executive Officer can be contacted at PrivacyCommittee@sa.gov.au.

3.11. Access and Correction of Personal Information

Principles 5 and 6 of the IPPI outline the requirement for agencies to provide individuals with a right to apply for access to their personal information and / or to seek to have it corrected under the *Freedom of Information Act 1991*, if they consider it to be incomplete, incorrect, out-of-date or misleading.

Any access / amendment request should be handled by an accredited FOI Officer. Further advice can be found on the State Records website.

4. Monitoring and reporting

1. Commitment to personal information privacy

2. Education

3. Privacy Policies and Practices

4. Monitoring and Reporting

It is recommended to regularly monitor and review information privacy processes and practices. This will ensure they remain fit for purpose and achieve continuous improvement. It will also build on your agency’s privacy maturity and capability.

Annual reviews and audits to monitor, review and improve the protection of information privacy can be conducted.

UNDER DEVELOPMENT

State Records is developing a tool to assist in self-assessment to evaluate privacy maturity and capability. It is similar to the tool provided for self-assessment against the Information Management Strategy and Standard.

After self-assessment, each agency can develop a plan to work on improving the privacy maturity.

4.1. Self-Assessment Tool

The aims of self-assessment are to rate against key information privacy measures and identify areas for improvement, resulting in an assessment of privacy maturity.

The self-assessment tool will assist with:

- assessing commitment to and respect for personal information privacy
- assessing how personal information in the agency is managed
- measuring how proactive the agency is in protecting personal information
- assessing compliance with the Information Privacy Principles Instruction
- assessing compliance against key privacy and information access requirements
- identifying areas where improvements are required
- developing a privacy management plan to improve information privacy requirements in the agency, and
- generating reports detailing agency maturity and capability levels.

The tool offers a scalable approach, over four levels, to identify areas of strength and weakness for a range of privacy measures.

0	**Absent**	The agency is either unaware of information privacy or has taken no steps to implement the protection of information privacy.
1	**Basic**	The agency has an awareness of its information privacy obligations but there is little practical evidence of action. Planning has commenced.
2	**Operational**	The agency is actively addressing information privacy. There is evidence of a planned approach, even if it is not fully implemented in some areas.
3	**Proactive**	The agency has a dedicated commitment to achieving the protection of personal information through privacy by design measures implemented throughout the agency and ongoing monitoring and review.

The higher the level of maturity and capability, the greater an agency's commitment to protecting personal information and the more privacy measures are proactively incorporated into the day-to-day operations agency.

Conversely, the lower the maturity and capability level, the greater the opportunity to implement and improve information privacy measures.

Reports from the tool can be used to brief senior management on progress towards implementing methods of protecting information privacy and the measures that can be taken to improve existing protection.

Your agency's risk profile may influence your decisions relating to what maturity level it seeks to achieve. For example, is your agency a low-risk agency, or a high-risk agency, or somewhere in between?

To decide on your agency's risk profile, consider your agency's obligations, its services, activities and functions, the type of personal information it holds and how much, the size and resources of the agency.

If your agency is largely policy focussed, doesn't manage much, if any, personal information and doesn't provide public services, your agency's risk profile may be low and so may decide a basic or operational level achievement is sufficient. Conversely, if your agency provides considerable public services with significant personal information involved, the risk profile may be considered high and a proactive level is required to ensure a robust information privacy framework is achieved.

Benchmarking

Though not mandatory, your agency is encouraged to report all self-assessment results to State Records.

The results will be used for the purposes of benchmarking and analysis. The aim is to record the improvements to information privacy in agencies over time.

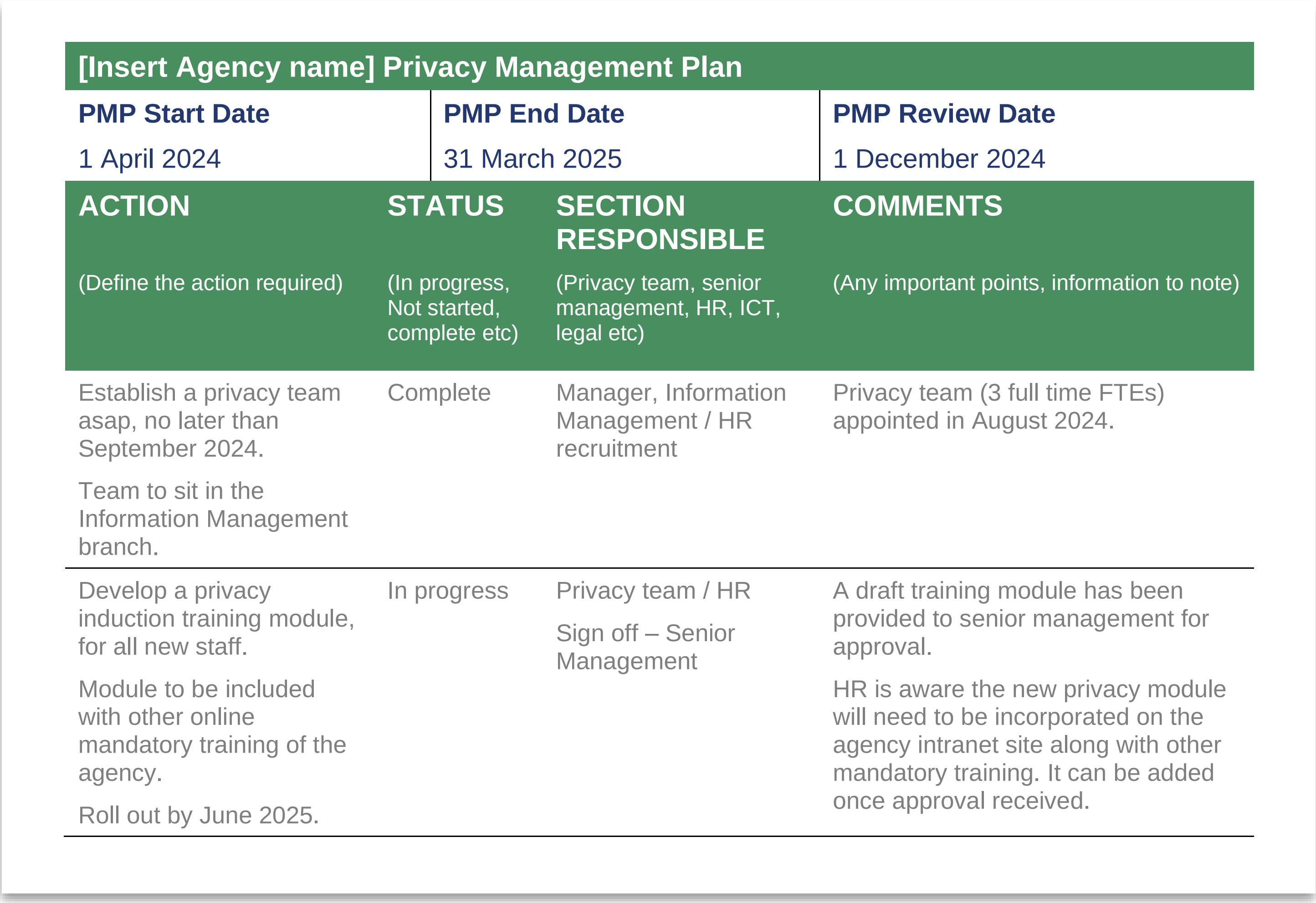
In addition, the results may help to identify any gaps in policy or advice State Records provides to further improve the protection of individual privacy in South Australia.

4.2. Privacy Management Plan

Once a self-assessment has been conducted, it can inform the development of a privacy management plan (PMP).

A PMP identifies specific, measurable privacy goals and targets and sets out how to achieve a path to privacy maturity.

A PMP might look something like this:



[Insert Agency name] Privacy Management Plan

PMP Start Date	PMP End Date	PMP Review Date
1 April 2024	31 March 2025	1 December 2024

ACTION (Define the action required)	STATUS (In progress, Not started, complete etc)	SECTION RESPONSIBLE (Privacy team, senior management, HR, ICT, legal etc)	COMMENTS (Any important points, information to note)
Establish a privacy team asap, no later than September 2024. Team to sit in the Information Management branch.	Complete	Manager, Information Management / HR recruitment	Privacy team (3 full time FTEs) appointed in August 2024.
Develop a privacy induction training module, for all new staff. Module to be included with other online mandatory training of the agency. Roll out by June 2025.	In progress	Privacy team / HR Sign off – Senior Management	A draft training module has been provided to senior management for approval. HR is aware the new privacy module will need to be incorporated on the agency intranet site along with other mandatory training. It can be added once approval received.

Actions can be linked back to sections of the self-assessment and can be endorsed by senior management.

A SMART goal framework, to set goals for the PMP, ensures the goals and targets are clearly defined, are realistic and achievable, with set deadlines.

Once developed and approved, the PMP should be disseminated to the relevant sections / teams to ensure the goals and targets are actioned and implemented.

PMPs should be reviewed and updated to ensure goals and targets are achieved or carried over, and to include any new issues raised through PIAs or other assessments.

SMART Goals

- *Specific* – well defined, clear and easy to understand
- *Measurable* – with specific criteria that measure your progress towards achievement
- *Achievable* – attainable and not impossible to achieve
- *Realistic* – relevant to the purpose within reach
- *Timely* – with a clearly defined timeline e.g. a start date and a target date.

Date approved	Approved by	Date for review	Version
28/06/2023	Director, State Records	28/06/2023	1

Need further assistance?

State Records
Tel (+61 8) 7322 7077
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au