

8.1 REVIEW OF POLICY NO. 4.1.31 - PRIVACY MANAGEMENT

- Attachments:**
1. **Policy No. 4.1.31 - Privacy Management**
 2. **Readiness Guide 10 - Privacy Policy**
 3. **Assessment of Policy No. 4.1.31 - Privacy Management**

RECOMMENDATION

That Council REPEAL Policy No 4.1.31 – Privacy Management at Attachment 1.

PURPOSE OF REPORT:

To seek Council's consent to repeal Policy No. 4.1.31 – Privacy Management at **Attachment 1**.

DELEGATION:

Section 2.7 of the *Local Government Act 1995* sets out the Role of Council as being to 'determine the local government's policies'. There is no delegation to Administration to make, review or repeal policies.

BACKGROUND:

The [Privacy Management Policy](#) (Policy) was adopted by Council in November 2010 with no amendments since adoption.

The Policy was developed due to a lack of privacy legislation in Western Australia and provides guidelines for Administration when dealing with personal information.

The Privacy and Responsible Information Sharing (PRIS) Bill was first introduced to the Western Australian Parliament in March 2023. The Bill is designed to introduce Information Privacy Principles (IPPs) and create a legislative framework to improve how public sector entities handle personal information. It also aims to facilitate responsible information sharing within the public sector while maintaining privacy protections for individuals.

In 2022, Administration initiated a review of the Policy in anticipation of the new privacy legislation however, this was postponed due to the impending guidance documents that were being developed by the Office of Digital Government (DGov).

DETAILS:

A Baseline PRIS Readiness Assessment Tool and Readiness Guides were developed by DGov in early 2024. In response to Readiness Guide 10 - Privacy Policy (at **Attachment 2**), Administration has recommenced this review.

The elements set out in clause 1.3 of the Policy Development and Review Policy have been considered as set out below.

Requirement for a documented City position (including community need or legislative requirement):

There is currently no legislative requirement for this Policy however the City recognises that there are reasonable risks associated with a lack of documented guidance on how it handles the personal information it collects, holds, uses and discloses.

The existing Policy is out of date and refers to superseded National Privacy Principles.

Explicit references to the provisions of the PRIS Bill cannot be included in a policy until the relevant provisions (the IPPs) come into force.

The Australian Privacy Principles (APPs) were introduced under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amended the *Privacy Act 1988*. They were published by the Office of the Australian Information Commissioner (OAIC) and came into effect on 12 March 2014.

These principles form the cornerstone of privacy law in Australia, guiding how organisations manage personal information. Although they do not directly apply to Local Government agencies, they offer valuable insights on best practices for handling personal information.

Administration is proposing to repeal the existing Council Policy and develop an Administrative Standard that aligns with the APPs while waiting for the PRIS Bill to be passed. An Administrative Standard will provide flexibility to incorporate the impending legislative change in a timely manner while continuing to provide essential guidance and prepare for privacy law reform.

A review of the current policy provisions and impact of repealing has been provided in **Attachment 3**.

Examples of current/best practice:

Administration is recommending that the Policy is repealed and replaced with an updated Administrative Standard that aligns with the Australian Privacy Principles being [APP 1](#) to [APP 13](#).

The APPs cover important areas such as:

- **Transparency and open management** of personal information (APP 1),
- **Collection and consent** requirements (APPs 3, 5),
- **Use and disclosure** of personal information (APP 6),
- **Access and correction** of data (APPs 12, 13).

By incorporating these principles, guidance would be provided to Administration that is align to Commonwealth legislation as an interim measure until WA-specific privacy legislation is enacted.

This step would also support compliance with the Office of Digital Government's readiness plan.

CONSULTATION/ADVERTISING:

No community consultation is required for the repeal of the policy.

LEGAL/POLICY:

Section 2.7(2)(b) of the *Local Government Act 1995* provides Council with the power to determine policies.

The City's Policy Development and Review Policy sets out the process for the development and review of the City's policy documents.

RISK MANAGEMENT IMPLICATIONS

Low: It is low risk for Council to repeal the policy as the policy is proposed to be replaced with an Administrative Standard that aligns with the APPs while waiting for the PRIS Bill to be passed.

An Administrative Standard will provide flexibility to incorporate the impending legislative change in a timely manner while continuing to provide essential guidance and prepare for privacy law reform.

Council at its meeting 15 December 2020 resolved to adopt the Policy Development and Review Policy to guide administration on the development and review of the City's strategies, policies and action plans to achieve transparent and consistent decision making which align with the City's objectives, strategic priorities and legislative requirements.

This policy includes the local government decision making hierarchy on page 2 which identifies that a Policy is adopted by Council and is the general rule or principle which is required to provide clear direction to Administration on the day to day management of the City.

The *Local Government Act 1995* at section 5.41(c) and (d) outlines the Functions of Chief Executive Officer are to:

- (c) *cause council decisions to be implemented; and*
- (d) *manage the day to day operations of the local government;*

As Privacy Management will be informed by State based legislation there is no requirement for a council adopted position and an Administrative Standard is in line with what is intended by the Privacy and Responsible Information Sharing (PRIS) Bill.

STRATEGIC IMPLICATIONS:

This is in keeping with the City's *Strategic Community Plan 2018-2028*:

Connected Community

We are an inclusive, accessible and equitable City for all.

Innovative and Accountable

We are open and accountable to an engaged community.

SUSTAINABILITY IMPLICATIONS:

This does not contribute to any environmental sustainability outcomes. This action/activity is environmentally neutral.

PUBLIC HEALTH IMPLICATIONS:

This does not contribute to any public health outcomes in the *City's Public Health Plan 2020-2025*.

FINANCIAL/BUDGET IMPLICATIONS:

Nil.

POLICY NO: 4.1.31**PRIVACY MANAGEMENT****OBJECTIVES**

The objectives of this Policy are:

- to ensure that *Personal Information* is collected, accessed, used, stored, and disposed of in accordance with the *Privacy Act 1988 (Cwth)* and *Privacy Amendment Act 2004 (Cwth)*; and
- to provide guidelines for the City when dealing with information.

POLICY STATEMENT

The City of Vincent respects every individual's right to privacy, dignity and confidentiality.

In order to comply with the requirements of the Acts and Regulations governing the action of local government, the City of Vincent will provide appropriate information to the public, in accordance with this Policy, the *Local Government Act 1995* and other relevant legislation.

PRIVACY ACT 1988

"*Personal Information*" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

"*Sensitive Information*" means:

(a) information or an opinion about an individual's:

- (i) racial or ethnic origin; or
- (ii) political opinions; or
- (iii) membership of a political association; or
- (iv) religious beliefs or affiliations; or
- (v) philosophical beliefs; or
- (vi) membership of a trade union; or
- (vii) sexual preference or practices; or
- (viii) criminal record;

that is also *Personal Information*; or

(b) health information about an individual.

PRIVACY PRINCIPLES

As at November 2010, Western Australia does not have specific privacy legislation which applies to local government. However, wherever possible, the City of Vincent will endeavour to comply with Commonwealth legislation.

In relation to the *Privacy Act 1988 (Cwth)* and *Privacy Amendment Act 2004 (Cwth)*, the City of Vincent will endeavour to always comply with the National Privacy Principles, as follows:

1. NATIONAL PRIVACY PRINCIPLE 1 – COLLECTION

1.1 The City of Vincent will not collect Personal Information unless:

- (i) information is collected for a lawful purpose that is directly related to a function or activity of City of Vincent, and
- (ii) the collection of the information is reasonably necessary for the purpose.

The City of Vincent will not collect Personal Information by any unlawful means.

1.2 When collecting Personal Information, the City of Vincent will collect information only from the individual to whom the information relates unless:

- (i) the individual has authorised collection from someone else; or
- (ii) the information has been provided by a parent or guardian of a person under the age of 16 years.

1.3 When the City of Vincent collects Personal Information about an individual, that person will be notified of:

- (i) the fact that the information is being collected;
- (ii) the purposes for which the information is collected;
- (iii) the intended recipients of the information;
- (iv) whether the supply of information is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided;
- (v) the name of the organisation that will collect the information and the address where the information will be stored.

2. NATIONAL PRIVACY PRINCIPLE 2 – USE AND DISCLOSURE

2.1 The City of Vincent will not use Personal Information for a purpose other than for which it was collected unless:

- (i) the individual to whom the information relates has consented to use the information for that other purpose; or
- (ii) the other purpose for which the information is used is directly related to the purpose for which it was collected; or
- (iii) the use of the information or that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom that information relates or of another person.

2.2 Situations where the City of Vincent may use or disclose information without an individual's consent include where it:

- (i) reasonably believes that use or disclosure is necessary to reduce or prevent a threat to a person's life, health or safety or a serious threat to public health or safety;
- (ii) is investigating or reporting on suspected unlawful activity;
- (iii) reasonably believes that the use is necessary for law enforcement, public revenue protection, prevention and remedying of serious improper conduct, or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body.

Note: If the City uses or discloses information without consent, the City's Officer will make a written note of such disclosure.

2.3 The City of Vincent will take reasonable care not to disclose Personal Information unless:

- (i) the disclosure is directly related to the purpose for which it was collected and there is not reason to believe the individual concerned would object; or
- (ii) the individual has been made aware that this kind of information is usually released; or
- (iii) disclosure is necessary to prevent or lessen a serious or imminent threat to the life of the individual concerned or another person.

2.4 The City of Vincent will take reasonable care not to disclose Personal Information that:

- (i) relates to an individual's ethnic or race origin, political opinions, religion or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person;
- (ii) relates to any enquiry from anyone outside the State of Western Australia unless a relevant privacy law applies to *Personal Information* in force in that jurisdiction.

PUBLIC REGISTERS

The City will not disclose *Personal Information* kept in a Public Register unless the information is to be used for a purpose relating to the purpose of the Register, or an Act under which the Register is kept.

The City requires that any person who applies for information from a Public Register completes a statutory declaration describing the intended use of any information obtained from the public register.

3. NATIONAL PRIVACY PRINCIPLE 3 – DATA QUALITY

3.1 The City of Vincent will take reasonable steps to ensure that:

- (i) information collected is relevant to a purpose, is not excessive, and is accurate, up-to-date and complete and the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

4. NATIONAL PRIVACY PRINCIPLE 4 – DATA SECURITY

4.1 With regards to the retention and security of Personal Information, the City of Vincent will ensure:

- (i) that information is used for a lawful purpose and is kept for no longer than is necessary;
- (ii) that the information will be disposed of securely;
- (iii) that the information is protected against loss, unauthorised access, use, modification or disclosure and against all other misuse (as are reasonable in the circumstances);
- (iv) if it is necessary to release the information to a person in connection with the provision of a service to the City of Vincent, everything reasonable is done to prevent unauthorised use or disclosure of the information by the service provider; and
- (v) all *Personal Information* will be stored securely.

4.2 The culling and destruction of records is carried by the City's Senior Records Officer in accordance with the *State Records Act 2000*, City of Vincent Record Keeping Plan and General Disposal Authority for the Local Government Records.

5. NATIONAL PRIVACY PRINCIPLE 5 – OPENNESS

The City of Vincent will be open and accountable about how it manages *Personal Information*.

6. NATIONAL PRIVACY PRINCIPLE 6 – ACCESSING AND CORRECTING PERSONAL INFORMATION

Access may be requested by an individual to correct the information if they believe that it is incorrect, incomplete or out of date.

Usually, when asked, the City will give an individual access to their *Personal Information*, unless there is a reason why the City cannot do so.

6.1 If the City of Vincent holds Personal Information about any individual it must take the necessary steps to enable any person to ascertain:

- (i) whether the City of Vincent holds *Personal Information*; and
- (ii) whether the City of Vincent holds *Personal Information* relating to that person; and
- (iii) if the City of Vincent holds *Personal Information* relating to that person:
 - (a) the nature of that information; and
 - (b) the main purposes that the information is being used; and
 - (c) that person's entitlement to gain access to that information.

6.2 Any person will be able to ascertain whether the City of Vincent holds their Personal Information by submitting a written request.

6.3 Any person who is not satisfied with the accuracy or acceptable use of their Personal Information kept by the City of Vincent may request amendments be made to that information by writing to the Chief Executive Officer

- (i) *Personal Information* must be used for the purpose that it was collected, and used for any purpose that is directly related to the purpose. It must be relevant, up-to-date, complete and not misleading.
- (ii) it will require appropriate supporting documentation, for example, a marriage certificate or statutory declaration.
- (iii) The City of Vincent has an obligation to take steps to amend *Personal Information* where necessary. If the City of Vincent decides that it will not amend the information, it must add the additional information, so it can be read with the existing information and the individual notified. The individual to whom the information relates is entitled to have the recipients notified of the amendments made by the City of Vincent.

6.4 The City of Vincent will take reasonable steps to ensure the accuracy of Personal Information prior to use, having regard to the purpose it was collected, its proposed use, its relevance, accuracy, whether it is up-to-date, complete and not misleading.

7. REVIEW OF CERTAIN CONDUCT (INTERNAL REVIEW PROCESS)

7.1 Where a person who has requested information is aggrieved by the conduct of the City of Vincent, as for example, in the following circumstances:

- (i) contravention of a privacy principle that applies to the City of Vincent;
- (ii) contravention of a Code of Practice that applies to the City of Vincent; and
- (iii) disclosure of *Personal Information* kept on a public register.

the person (Applicant) is entitled to apply for an Internal Review.

The application for a review must be in writing and addressed to:

Chief Executive Officer
City of Vincent
244 Vincent Street
Leederville WA 6007

The application must be submitted no later than 6 months from the time the Applicant first becomes aware of the conduct (the subject of the application).

7.2 The application will be dealt with by the Chief Executive Officer who will consider any relevant material submitted by the applicant.

The review will be completed as soon as reasonably practicable and within 60 days from receipt of the application for review. Following completion of the review, the City of Vincent may do one or more of the following:

- (a) take no further action on the matter;
- (b) make a formal apology to the applicant;
- (c) take appropriate remedial action;
- (d) provide undertakings that the conduct will not occur again;
- (e) implement administrative measures to ensure that the conduct will not occur again; or
- (f) any combination of the above.

7.3 As soon as practicable within 14 days of the completion of the review, the City of Vincent will notify the applicant in writing of:

- (i) the findings and the reasons for those findings;
- (ii) any proposed action to be taken; and
- (iii) the right of the applicant to have those findings.

7.4 Refusing a Request

- (i) The City may deny a request for access if the Chief Executive Officer reasonably believes:
 - (a) it would pose a serious or imminent threat to the life or health of any person;
 - (b) the privacy of others would be unreasonably affected;
 - (c) the request is frivolous or vexatious;
 - (d) the information relates to existing legal proceedings with the person who is the subject of the information and would not be accessible through discovery;
 - (e) providing access would prejudice negotiations with the person who is the subject of the information by revealing the City's intentions regarding those negotiations;
 - (f) providing access would be unlawful or denying access is required or authorised by law;
 - (g) providing access would be likely to prejudice an investigation of unlawful activity or law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body; or
 - (h) an enforcement body performing a lawful security function requests denial of access to protect national security.
- (ii) If the City refuses access, it will usually explain why.
Access may be by providing the individual with a copy of the information or by review of the information with the management at the City.

8. NATIONAL PRIVACY PRINCIPLE 7 – IDENTIFYERS

The City will generally not adopt Commonwealth Government identifiers, such as Tax File Number or Medicare Numbers for use as its own identifiers. If the City is required to collect a government identifier in providing services to individuals, it will not use this number to identify the individual.

9. NATIONAL PRIVACY PRINCIPLE 8 – ANONYMITY

Where requested and reasonably possible, the City will give individuals the option of dealing with the City anonymously.

10. NATIONAL PRIVACY PRINCIPLE 9 – TRANSBORDER DATA FLOW

This principle mainly relates to the transfer of information overseas and is not applicable to the activities of the City. However, the City will not disclose information, unless required by law.

11. NATIONAL PRIVACY PRINCIPLE 10 – SENSITIVE INFORMATION

The City will not collect '*Sensitive Information*' about an individual, except where:

- (a) the collection is required by law or to establish, exercise or defend a legal or equitable claim; or
- (b) it is necessary to prevent or lessen a serious or imminent threat to the life or health of the person who is the subject of the information; or
- (c) it is legally required to assist in providing a wider range of services to the community.

12. CODE OF CONDUCT

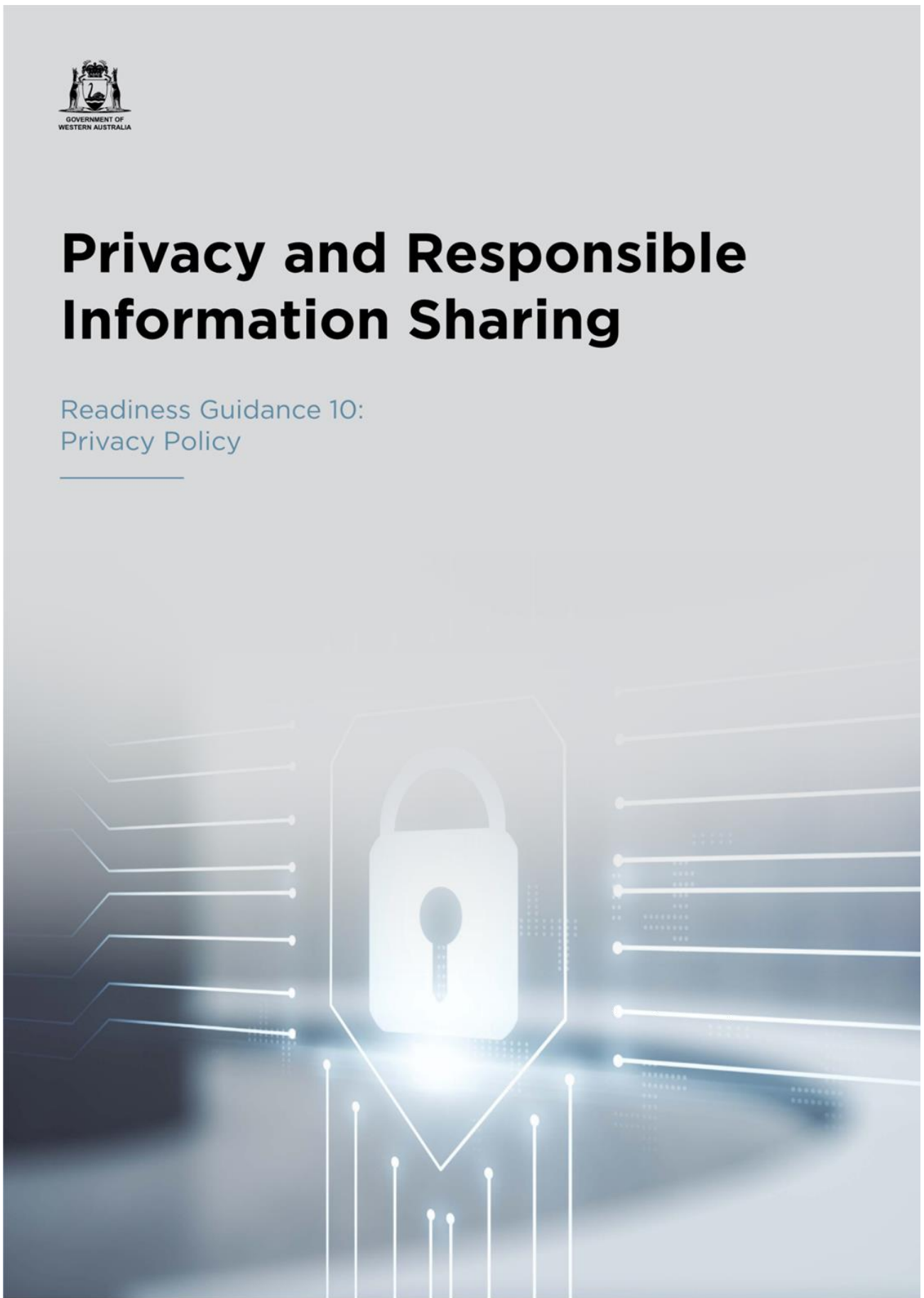
Part 7 of the Council's Code of Conduct outlines Council Member and Employee obligations in relation to "Access to Information".

Date Adopted:	November 2010
Date Amended:	-
Date Reviewed:	-
Date of Next Review:	November 2015



Privacy and Responsible Information Sharing

Readiness Guidance 10:
Privacy Policy



Introduction

The WA Government has drafted new legislation that will form the basis of Privacy and Responsible Information Sharing (PRIS) reforms. These reforms build on an extensive consultation process that commenced in 2019 to develop a model that is right for Western Australia.

Your agency is to develop and publish a Privacy Policy, describing how it handles personal information.

Agency PRIS Readiness Plan and Checklist

An Agency PRIS Readiness Plan has been developed to help agencies prepare for and implement the legislation. The Readiness Plan describes the approach, governance, key activities, deliverables and milestones to ensure agencies are prepared to meet both the privacy and responsible information sharing requirements of the PRIS legislation once it commences.

The aim of the Readiness Plan is to ensure your staff and supporting personnel:

- » understand and are engaged with the process of reform;
- » are prepared and capable of complying with the proposed privacy provisions; and
- » are ready to meet the responsible information sharing provisions within the PRIS legislation.

The Agency PRIS Readiness Checklist supports the Readiness Plan and provides a snapshot of the readiness actions. It includes a timeline of five self-assessment and reporting activities, and 18 key actions required for PRIS readiness by the time the legislation comes into force.

The Checklist outlines the minimum policies and processes an agency should have in place (it does not include all the actions from the Readiness Plan). These actions are based on established best practices for information management and are not dependent on the new legislation.

The WA Government has provided the authorising environment for agencies to prioritise this program of activities by June 2025.

Key Action 8: Develop and publish a Privacy Policy

This is the eighth action in the Agency PRIS Readiness Checklist.

Agencies develop and publish a Privacy Policy, describing how they handle personal information, by **30 September 2024**.



Purpose

The PRIS legislation establishes a framework that strengthens privacy protections for Western Australians and introduces Information Privacy Principles (IPPs) to govern the handling of personal information by IPP entities.

This guide is designed to help agencies develop and maintain a publicly available Privacy Policy aligned with IPP 5 Openness and Transparency.

Agencies may also develop internal policies and procedures that offer more detailed guidance to staff about their responsibilities and how to handle personal information in the course of their duties.

You should read this guide together with the full text of the IPPs and Part 2 of the PRIS legislation.

What is a Privacy Policy?

The PRIS Bill introduces 11 IPPs that govern the collection, use, disclosure and security of personal information.

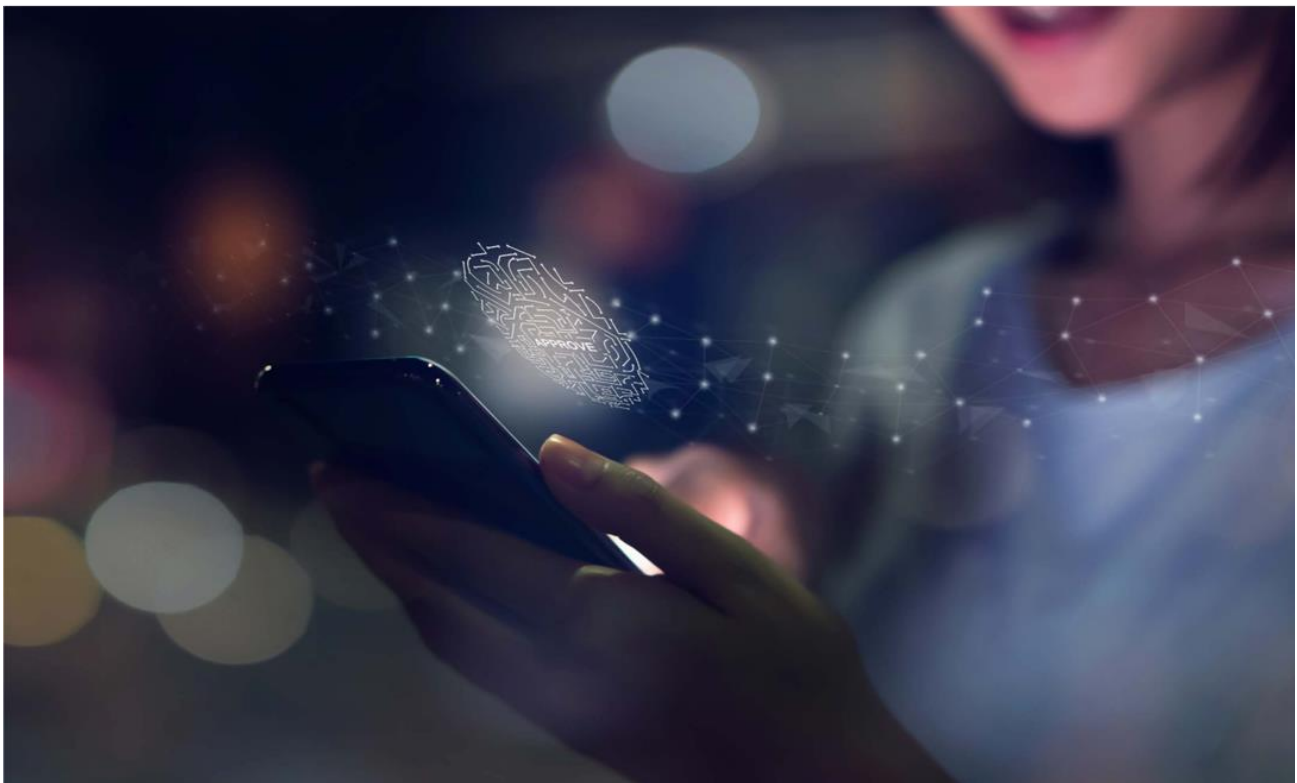
IPP 5: Openness and Transparency requires an IPP entity to develop a document that clearly sets out its policies on the handling of personal information, and to make the document available to anyone who asks for it.

This document is commonly referred to as a Privacy Policy.

A Privacy Policy is an important document to inform customers, clients and stakeholders how your agency handles the personal information it collects, holds, uses and discloses.

A Privacy Policy is an important statement about how your agency handles personal information. It demonstrates your agency's commitment to protect the privacy of personal information and promotes public confidence.

A concise and easy to read Privacy Policy helps to demonstrate your agency's commitment to protecting the privacy of personal information by explaining how it meets its privacy obligations.



Why is a Privacy Policy required?

A Privacy Policy is required by **Information Privacy Principle 5: Openness and Transparency**.

An open and transparent Privacy Policy helps build trust with your agency's customers, clients and stakeholders by keeping them informed about how your agency handles personal information. It gives people confidence that your agency collects, uses and discloses personal information in accordance with the privacy protections contained in the IPPs.

As a clear expression of your agency's intentions, a Privacy Policy provides direction to staff about their obligations to handle personal information according to the requirements of the PRIS legislation. It helps staff understand the context for their responsibilities and expected behaviours, building a privacy-aware organisational culture.

In addition to meeting the requirements of IPP 5, other benefits of having a Privacy Policy include:

- » supporting your agency to handle personal information in accordance with the PRIS legislation;
- » informing staff about the new PRIS legislation and providing key messages about their responsibility to handle personal information appropriately;
- » helping to prevent unauthorised collection, use or disclosure of personal information;
- » providing a framework to assist your agency when responding to a privacy complaint; and
- » promoting public confidence in your agency's handling of personal information.

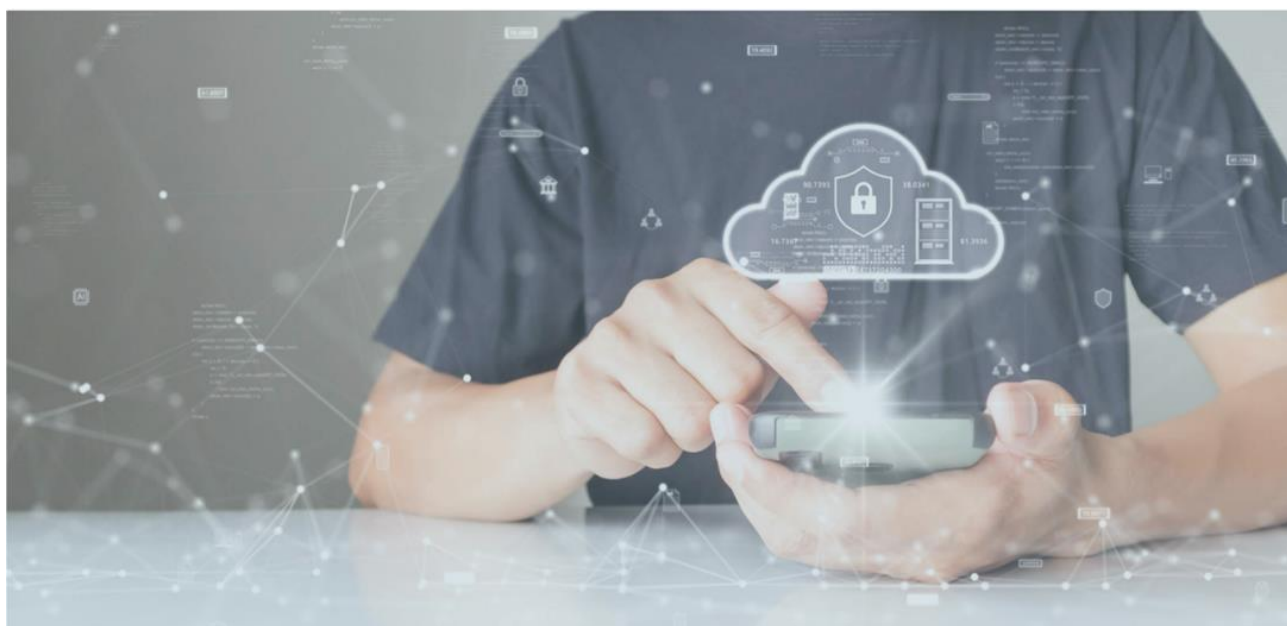


Figure 1 sets out the full text of IPP 5.

Principle 5: Openness and Transparency

- 5.1 An IPP entity must develop a document setting out policies on its handling of personal information and must make the document available to anyone who requests it.
- 5.2 A document referred to in subclause 5.1 must be up-to-date, clear, concise and expressed in plain language.
- 5.3 On request by a person, an IPP entity must take reasonable steps to let the person know, generally -
- (a) the kinds of personal information that the IPP entity collects and holds; and
 - (b) how the IPP entity handles personal information; and
 - (c) the purposes for which the IPP entity handles personal information; and
 - (d) whether any personal information held by the IPP entity is used for an automated decision-making process.

Figure 1: Information Privacy Principle 5 (IPP 5)



What should a Privacy Policy contain?

At a minimum, a Privacy Policy should include:

- » the date and version number of the policy;
- » the identity of the agency;
- » who in the agency is the officer responsible for the Policy;
- » the agency's main functions;
- » the types of personal information the agency generally collects and holds to fulfil its main functions;
- » how the agency collects personal information (including, for example, the use of cookies on the agency's website);
- » whether the collection of personal information is compulsory or optional (including referring to any relevant legislation that authorises the collection, use or disclosure of the information);
- » the purposes for which the agency uses and discloses personal information;
- » how the agency will use and disclose the personal information it collects, including the types of third parties the personal information may be disclosed to;
- » whether any personal information is used for an automated decision-making process;
- » how the agency handles unique identifiers;
- » whether the agency has processes to de-identify personal information and if so, how the de-identification is undertaken and how the de-identified information is handled;
- » how the agency ensures the personal information is securely stored and for how long it may be stored;
- » how the privacy of personal information is protected if it is transferred or stored outside Australia;
- » how the agency controls and manages access to personal information; and
- » how an individual can contact the agency, request access to the information held about themselves, or make a privacy complaint.

Your agency may have an existing Privacy Policy. If so, it should be reviewed and updated, or replaced, to ensure it meets the requirements of the PRIS legislation and supports your agency to handle personal information appropriately.

A Note of Caution

Agencies should take care not to make explicit references to the provisions of the PRIS Bill in the Privacy Policy, until the relevant provisions (the IPPs) come into force

Privacy Policies and Collection Notices

Although they both inform individuals about how an agency will handle their personal information, Privacy Policies and Collection Notices are different.

A Privacy Policy speaks about an agency's practices for handling personal information in a broad sense.

A Collection Notice outlines an agency's information handling practices for a specific purpose or activity.

Example

When collecting personal information from an individual who is registering their pet, a local council will provide the pet owner with a notice about how it will handle that specific information.

This is different to the council's Privacy Policy, which will outline the council's commitment to handle personal information in accordance with the IPPs in a more general sense.

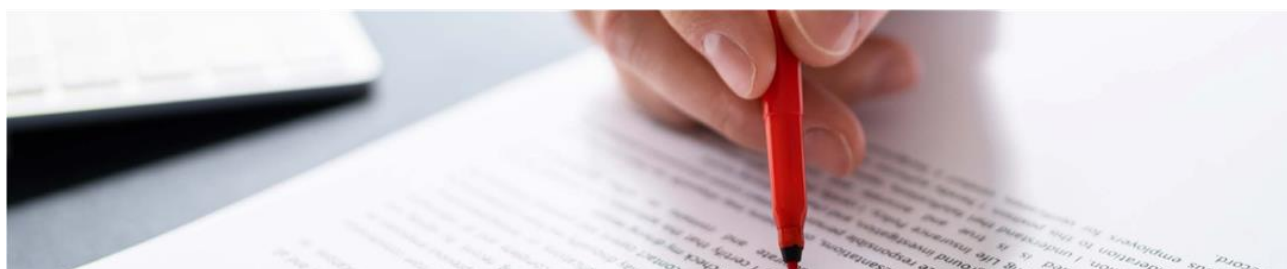
The requirements for a Collection Notice are provided in IPP 1.9 and further information will be included in **Readiness Guidance 13**.

Tips to keep in mind

Although every agency's Privacy Policy must contain the information outlined in IPP 5, they don't need to look and read the same. Here are some tips to help make your Privacy Policy genuinely informative and helpful for your audience.

More details are provided in the following section, which outlines the steps to develop your Privacy Policy.

*Use plain language, short, clear sentences and
avoid legal jargon or technical words.*





Tips for developing your Privacy Policy

- ~ Consider your audience. Don't treat your Privacy Policy as a legal document to manage legal risk. Create trust in your agency by genuinely speaking to your customers, clients or stakeholders.
- ~ Use your own words. Your Privacy Policy shouldn't just restate the IPPs. It should demonstrate the steps that your agency will take to comply with the IPPs.
- ~ Make it specific to your agency's business or operations. Think about what your agency does (its core functions and activities) and how it handles personal information to do it.
- ~ Consult before drafting. Identify whether your agency has an existing Privacy Policy. Speak to all areas of your agency, including your communications team, to seek feedback on what should be included in your Privacy Policy and how best to communicate it to your audience. There might be innovative ways to do this, such as infographics or videos. Speak to your in-house legal team or contact the State Solicitor's Office if you require legal advice.
- ~ Focus on what's important. Don't attempt to include every tiny detail. Don't re-state obligations that appear in other policies or legislation. Include references or links as appropriate.
- ~ Use a layered approach. For example, provide a summary version of the key matters in your Privacy Policy on your website, with a link to the full document.
- ~ Keep it simple. Use simple language, as required under IPP 5.2. Test the readability of the content and format with your communications area. Make sure the document is accessible by all audiences.
- ~ Think about the different technologies your agency uses. Your general Privacy Policy doesn't need to be technology specific. However, you might want to include specific sections, or create standalone policies about your agency's use of particular technologies. For example, your Privacy Policy could contain a distinct section about your agency's handling of personal information collected via its website, or you may choose to develop a separate website Privacy Policy.
- ~ Is one Privacy Policy enough? Depending on the range and diversity of its core functions, an agency may choose to publish more than one Privacy Policy. If your agency is large or complex with different operating environments, you should consider whether you need more than one Privacy Policy.



Steps to develop your Privacy Policy

The IPPs are principles rather than detailed rules. They are outcomes-focused, which enables them to be applied flexibly and adapted to the different operating environments.

Consider the following practical steps to develop a Privacy Policy.



Step 1. Gather the right information

The key to developing a Privacy Policy is to have an overview of the personal information held by your agency, as well as your personal information handling practices, procedures and systems. This will enable you to accurately describe (and summarise) how your agency handles personal information.

You may have gathered some of this information already, for example as part of your agency's existing Privacy Policy or in an Information Asset Register. If you have not yet gathered any of this information, consider conducting an information survey and make a list of the personal information held by your agency and any relevant policies and procedures. **Readiness Guidance 8** provides more suggestions for conducting an information survey.

Clearly describe your agency's functions and activities

To be able to write a Privacy Policy (or to review and update an existing Privacy Policy), you should be able to describe your agency's functions and activities and understand your agency's personal information handling procedures.

You should be able to describe your agency's main functions and activities and identify those that involve personal information handling. For example:

- » The provision of specific services
- » Handling complaints
- » Managing employee records
- » Operating your website

For each function or activity, you should be able to describe:

- » What personal information your agency collects and holds
- » How your agency collects and holds that personal information
- » What personal information your agency uses and discloses
- » Why your agency collects, holds, uses and discloses that personal information
- » Whether your agency discloses personal information to overseas entities

Understand your agency's personal information handling procedures

You should understand your agency's current personal information handling practices, procedures and systems (written or otherwise), for your agency as a whole, and for each of its key functions and activities including:

- » specific approaches, principles or commitments your agency has decided to adopt for handling particular types of personal information or in relation to a particular process

Example

If an agency collects personal information about equity markers for its clients, is that information:

- ~ linked across all business processes and systems; or
 - ~ linked only in certain, specified circumstances; or
 - ~ linked only with the client's consent; or
 - ~ never linked.
-
- » processes for identifying, assessing and managing privacy and security risks, as well as developing and monitoring controls for those risks
 - » security protections (for example, encryption, audit and monitoring) your agency has in place
 - » approaches to identifying and handling personal information your agency no longer needs. For example, your agency's practices under the *State Records Act 2000* (WA)
 - » how and why personal information is used by your agency for automated decision-making processes (if applicable)
 - » processes for providing access to and correction of personal information (refer to existing procedures for handling requests under the *Freedom of Information Act 1992* as applicable)
 - » complaints handling processes
 - » policies relevant to your agency's personal information handling. For example, your agency's approach to maintaining the quality of personal information that is used and disclosed, anonymity or pseudonymity
 - » policies for managing contractors when personal information may be disclosed
 - » alignment with other agency policies or procedures which relate to the collection, storage, use or disclosure of information. (For example, research data, appropriate use of technology; security and access restrictions; complaints handling.)

Your agency's Privacy Policy does not have to include all of the above information. However, understanding your agency's personal information handling practices procedures and systems will enable you to identify what is going to be most important to readers and work out what your Privacy Policy should focus on in detail, or summarise, or link to existing documents under a heading "Related Documents".



Step 2. Work out the content and structure

Although your Privacy Policy must cover the topics outlined in IPP 5, the information doesn't have to be presented in that order. The goal is to make it as easy as possible for individuals to find the information that is most important to them.

Arrange information in a way that makes sense

You should arrange the information in a way that makes sense for your agency's functions, activities and audience. For example, you could separate out personal information flows for particular groups for whom your agency has different information handling practices.

If you decide to have more than one Privacy Policy, make the scope of each policy clear and, if practical, explain how each Policy links to the others.

Focus on what is likely to be most important to your clients, customers and stakeholders

Focus more on the areas of personal information handling that individuals are:

- » Most concerned about or may find objectionable.

Example

Why the agency collects personal information such as date of birth or health information. How is the agency going to protect that personal information? Does the agency disclose personal information without the individual's knowledge or consent? Does the agency use the personal information to make automated decisions about the individual?

- » Unaware of, won't reasonably expect, or may not understand.

Example

Does the agency collect personal information about individuals from other sources? Does the agency track individual users on its website? If so, what does the agency use the information for? Can individuals interact with the agency anonymously or pseudonymously?

Be as specific as possible

Be specific about the way in which your agency handles personal information as this will provide clarity to internal and external stakeholders and build trust. Creating clarity and trust will be most important in areas of common concern such as contact details, health information, financial information or other sensitive personal information.

Unqualified use of vague words such as 'may' could lead to concern about uses and disclosures that are not intended.

Summarise where possible

Accurately summarise policy information in areas that:

- » Individuals know about already. For example, where they have provided personal information directly by filling out a form; or where a Collection Notice provides the detail.
- » Individuals would expect as common business or administrative practice for a particular transaction or service. For example, using an address for billing purposes or to enable a contractor to perform these services on behalf of the agency.
- » Are common across the agency for all personal information handling. For example, names or contact details.

Step 3. Provide information in layers

Take a layered approach to providing information about how your agency will handle personal information by providing a summary version (the summary Policy) that focuses on what the agency's clients, customers and stakeholders would like to know, with a link to a more complex and detailed Privacy Policy. This is particularly effective in the online environment.

Headings in the summary Policy may vary according to the particular functions and activities of your agency, but often include:

- » Scope — describes the range and extent of the Policy, the functions, business units, staff and systems covered by the Policy.
- » Collection of personal information — provides the key information about what personal information is collected and why. Focus on areas that are most sensitive or that clients, customers and stakeholders would least expect.
- » Disclosure (sharing) of personal information — describes the key uses and disclosures of personal information, the conditions around those disclosures, and why personal information is used or disclosed in this way. This is a good place to mention any overseas disclosures.
- » Requests and choices — describes any requests or choices that individuals can make, in relation to the handling of their personal information. For example, a choice to accept or reject cookies on a website, a choice to interact anonymously, or how an individual may request access to or correction of personal information the agency holds about them.
- » How to make a complaint — briefly describes how individuals can make a complaint about an alleged interference with their privacy and what the individual may do if they are not satisfied with the outcome.
- » Contact details — it may be helpful to provide the details of the agency's Privacy Officer. At a minimum, include a primary office telephone number and a general agency email address that won't change with personnel.

Try to keep the summary Policy to 500 words or less.

Step 4. Draft your Privacy Policy

Once you have a list of the personal information that your agency holds, as well as the other necessary information identified above, and have worked out the content and structure of your Privacy Policy, you can begin drafting.

Your Privacy Policy must be up-to-date, clear, concise and expressed in plain language, in accordance with IPP 5.2. To ensure the Policy is accessible, easy to navigate and easy to read:

- » Use the active tense (you, we, I) and simple language – no legal or government jargon or acronyms.
- » Use short sentences and break up text up into small, digestible paragraphs.
- » Use accessible, inclusive language and where possible provide alternative formats on request. For example, simple read, low vision alternative fonts or hardcopy.
- » Use headings to help people find information easily, including information that may particularly apply to individual situations or particular client, customer or stakeholder relationships with the agency.
- » Keep in mind how you are going to publish it. If it is going on your agency's website, make sure it is in a form suited to online publication and accessible to all readers.
- » Consider your main audience in the design and format of the Privacy Policy and/or the summary Policy. For example, if your audience is likely to view the summary Policy via a mobile app, you should create a document that works effectively in that format. Consider how the full Policy will be made publicly available to anyone who requests it, in accordance with IPP 5.1.
- » Avoid making it too wordy. Only include what is necessary and relevant to the way your agency handles personal information.
- » Make sure the Privacy Policy is readable. Web Content Accessibility Guidelines (WCAG) recommend the style and choice of words should be suitable for a lower secondary education reading level (year 7 or between 12 and 14 years old).

Step 5. Test your Privacy Policy

Test out your Privacy Policy and the summary Policy with the target audience or audiences, including likely readers. Where your resources are limited and systematic testing is not possible, try to identify a staff member who has not been involved in the development of the Privacy Policy – ask them to read the documents for clarity and to provide feedback. Regardless of the target audience, it should be able to be easily read and understood.

To ensure that the Privacy Policy and summary Policy cover all relevant topics and accurately reflect your agency's information handling practices, you could also test the documents with internal staff with responsibilities for handling personal information in the course of their regular duties.

Consider your agency's requirements for policy consultation and policy approval processes. For larger agencies, ensure the Privacy Policy is aligned with policy statements that apply to other areas of the organisation.

Step 6. Make your Privacy Policy available to anyone who requests it

The Privacy Policy should be accessible to everyone.

IPP 5.1 requires IPP entities to make their Privacy Policies available to anyone who requests it.

Although IPP 5.1 does not specifically require the Privacy Policy to be published, making a summary Policy readily available on your website will develop trust and reduce the workload associated with responding to individual requests.

This approach also aligns with the requirements of section 97 of the *Freedom of Information Act 1992* (WA), and the Open by Design Principles published by the Office of the Information Commissioner WA.

Note

If your agency is publishing its Privacy Policy before the requirements of the PRIS legislation come into force, include a clear statement at the beginning of the policy document, such as:

"The requirements of the Privacy and Responsible Information Sharing (PRIS) legislation have not yet commenced, but [the agency] has drafted this Privacy Policy in anticipation of the law coming into effect."

Step 7. Regularly review and update your agency's Privacy Policy

IPP 5.2 requires IPP entities to ensure their Privacy Policies are up-to-date. You should regularly review and update your Privacy Policy to ensure that it reflects your agency's current personal information handling practices.

When an agency adopts a new program, system or technology; is assigned new functions; or undergoes a restructure, it is worthwhile revisiting the Privacy Policy to ensure that it is still up to date and accurately reflects the flow of information through the agency.

If an agency begins to collect more information, or uses or discloses information in new ways, this should be immediately reflected in its Privacy Policy.

References

The information in this guidance is adapted from:

- » [Guide to developing an APP Privacy Policy](https://www.oaic.gov.au/privacy/privacy-guidance-for-agencies-and-government-agencies/more-guidance/guide-to-developing-an-app-privacy-policy), published by the Office of the Australian Information Commissioner (OAIC)
- » [Privacy Policies](https://ovic.vic.gov.au/privacy/resources-for-agencies/privacy-policies/), published by the Office of the Victorian Information Commissioner (OVIC)

The WA Government [Interim Privacy Position](https://www.wa.gov.au/government/announcements/interim-privacy-position) can be found at:

<https://www.wa.gov.au/government/announcements/interim-privacy-position>

The [Privacy and Responsible Information Sharing Bill](https://www.parliament.wa.gov.au/parliament/bills.nsf/BillProgressPopup?openForm&ParentUNID=3329DA2DC25F557148258B1E003267FF) can be found on the Parliament of Western Australia website, under Current Bills at:

<https://www.parliament.wa.gov.au/parliament/bills.nsf/BillProgressPopup?openForm&ParentUNID=3329DA2DC25F557148258B1E003267FF>

Examples of Privacy Policies:

- » Department of the Prime Minister and Cabinet (Cth) [Privacy Policy](https://www.pmc.gov.au/about-us/accountability-and-reporting/information-and-privacy/privacy-policy/full-version)
- » OVIC [Privacy Policy](https://ovic.vic.gov.au/about-us/internal-policies-procedures-and-registers/privacy-policy/)
- » OAIC [Privacy Policy](https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/plans-policies-and-procedures/privacy-policy)

Other useful resources include:

- » *Readiness Guidance 1: PRIS Champions*
- » *Readiness Guidance 6: Privacy Officers*
- » *Readiness Guidance 8: Information Survey and Information Asset Register*
- » The [Privacy Officer Toolkit](https://education.oaic.gov.au/privacy-officer-toolkit/), published by the OAIC.
- » [Privacy Officer Toolkit](https://ovic.vic.gov.au/privacy/resources-for-agencies/privacy-officer-toolkit/), published by the OVIC.
- » [Open by Design Principles](https://www.oic.wa.gov.au/en-au/About-Us/Open-Government/Open-by-Design-Principles), published by the Office of the Information Commissioner WA.

Information about [Privacy and Responsible Information Sharing](https://www.wa.gov.au/government/privacy-and-responsible-information-sharing) can be found at:

Please email privacy@dpc.wa.gov.au for further information about these resources.

Assessment of Privacy Management Policy (Policy No: 4.1.31)

Impact of Policy Repeal: The National Privacy Principles (NPPs) outlined in the current Privacy Management Policy are outdated and have been replaced by the Australian Privacy Principles (APPs). The repeal of this policy and its replacement with a proposed Administrative Standard will ensure alignment with the current legal framework as detailed below.

No.	Current Clause	Impact of Policy revocation
	Policy Statement	The current policy statement infers a legislative requirement to have a policy governing how the City manages information. However, there is no specific legislative requirement for a Council Policy. Compliance with the <i>Privacy Act 1988</i> and the Australian Privacy Principles (APPs) can be achieved through a proposed Administrative Standard, which will ensure that personal information is managed in accordance with current legal standards. This approach provides flexibility to incorporate the impending legislative change in a timely manner while continuing to provide essential guidance and prepare for privacy law reform.
Clause 1:	National Privacy Principle 1 - Collection	A proposed Administrative Standard will align with APP 3, ensuring personal information is collected only when necessary and by lawful means.
Clause 2:	National Privacy Principle 2 - Use And Disclosure	A proposed Administrative Standard will align with APP 6, ensuring personal information is used and disclosed only for the primary purpose or a related secondary purpose with consent.
Clause 3:	National Privacy Principle 3: Data Quality	A proposed Administrative Standard will align with APP 10, maintaining the quality of personal information.

No.	Current Clause	Impact of Policy revocation
Clause 4:	National Privacy Principle 4: Data Security	A proposed Administrative Standard will align with APP 11, ensuring evolving data security measures are in place.
Clause 5:	National Privacy Principle 5: Openness	A proposed Administrative Standard will align with APP 1, ensuring transparency in personal information management.
Clause 6:	National Privacy Principle 6: Access and Correction	A proposed Administrative Standard will align with APP 12 and APP 13, ensuring individuals can access and correct their personal information.
Clause 7:	Review of Certain Conduct (Internal Review Process)	Administrative procedures will continue to provide an internal review process, ensuring grievances related to privacy are addressed in accordance with the APPs.
Clause 8:	National Privacy Principle 7: Identifiers	A proposed Administrative Standard and supporting procedures will align with APP 9, ensuring the use of identifiers is compliant with current standards.
Clause 9:	National Privacy Principle 8: Anonymity	A proposed Administrative Standard will align with APP 2, providing options for anonymity.
Clause 10:	National Privacy Principle 9: Transborder Data Flow	A proposed Administrative Standard will align with APP 8, ensuring compliance responsible information sharing requirements.

No.	Current Clause	Impact of Policy revocation
Clause 11:	National Privacy Principle 10: Sensitive Information	A proposed Administrative Standard and supporting procedures will align with APP 3 and APP 6, ensuring sensitive information is handled appropriately.
Clause 12:	Code of Conduct	The City's Code of Conduct will continue to incorporate these obligations, ensuring continued compliance.