CITY OF Fremantle

Council Policy

Privacy Policy

fremantle.wa.gov.au

Privacy Policy

Policy scope

This policy sets out how the City of Fremantle manages the collection, storage and use of personal information (defined in this policy) to ensure documents that contain private information are appropriately managed. The Policy also outlines the requirements to manage and respond to an information breach and to mitigate risk of future breaches.

Policy statement

The City of Fremantle is committed to compliance with the obligations and requirements of the Privacy and Responsible Information Sharing legislation ('PRIS') and the Information Privacy Principles (outlined within schedule 1).

1. Personal information the City collects

1.1. An Individuals personal information will only be collected for purposes that relate to the City carrying out its functions as a local government.

1.2. The City collects personal information through the delivery of our services and functions, through correspondence, forms, service requests, and through online data and metadata collection.

1.3. The City may collect and use personal information of an individual for a secondary purpose other than what it was originally collected for or from another source, to perform the functions of the local government if it's required or authorised by or under law. The circumstances for this collection will be provided to the individual.

1.4. Collection notices will be provided to individuals within a reasonable timeframe in accordance with the PRIS Act when personal information is collected.

1.5. The City's Record Management Council Policy, and other internal policies and plans, may outline how personal information is managed, including but not limited to classification, retention, and breaches.

1.6. The City's privacy statement for the use of the City's corporate website is available here: https://www.fremantle.wa.gov.au/privacy-policy/. The City is not responsible for the collection of personal information by third parties which are accessed through links available on the City's website.

1.6.1. When visiting the corporate website, the City's internet service provider automatically records a user's visit and logs the following information for statistical purposes:

- The user's internet provider (IP) address
- The user's top level domain name (e.g. .com, .net, .gov ,etc.)

- the date and time of your visit to the site
- the pages accessed and documents downloaded
- time spent on individual pages
- time spent overall on the site
- browser type and version
- referring site (e.g. search engine)

This information is analysed regularly to determine the website's usage statistics.

1.6.2. No attempt will be made to identify a user or their browsing activities unless required by law, where a law enforcement agency may exercise a warrant to inspect the City's service provider's logs.

1.6.3. Where a user provides their email address and other personal information to subscribe to a City of Fremantle service via the website, all details will be used and maintained for the sole purpose of the mailing list or the activity they have been provided for. The user will have the option to unsubscribe from a mailing list service at any time. Their email address will remain confidential and no personal information will ever be disclosed to a third party without their explicit consent, unless required by law.

2. Personal information the City shares

2.1. The City will only use an individual's personal information for purposes that relate to the City carrying out its functions as a local government.

2.2. Personal information collected by the City will not be disclosed to a third party, unless:

a. The disclosure is a public interest disclosure, or it is information which the public has a right to access under relevant legislation;

b. The disclosure is required or authorised by or under any other law;

c. The individual concerned has consented to the disclosure;

d. The information is being utilised by a third party engaged on behalf of the City to undertake business purposes; or

e. The City 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.

2.3. The City will use processes to de-identify information by redacting out personal or confidential information as part of the Freedom of Information process and in accordance with the *Freedom of Information Act 1992.*

2.4. The City is required under the *Local Government Act 1995* and subsidiary legislation to make some personal information publicly available. A collection notice or applicable disclosure will be made when collecting the information.

2.5. The City will only disclose personal information outside of Australia in accordance with the PRIS Act.

3. Data Retention

3.1. The City is committed to safeguarding information against misuse, loss, modification and unauthorised access or disclosure.

3.2. Any records held by the City that contain personal information will be handled in a secure, responsible, and compliant manner. This includes the collection, storage, retention, and destruction of records.

3.3. The City will apply WA Information Classification policies for UNOFFICIAL, OFFICIAL, and OFFICIAL Sensitive information, and follow internal policies and guidelines to ensure the correct sensitivity and security measures are applied.

3.4. The City will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose, unless required or authorised to retain the information by law.

3.5. The City will comply with relevant legislation and internal policy in relation to data retention and disposal.

4. Data Breaches and Compliance

4.1. If a data breach occurs, the City will investigate the extent of the incident and ensure appropriate containment and mitigation measures are applied.

4.2. Affected individuals and regulatory bodies will be notified as required.

4.3. The City will provide regular training to employees in relation to their privacy responsibilities.

4.4. Individuals may report a breach to governance@fremantle.wa.gov.au or via the online service request portal.

5. Request for Personal Information

5.1. Customers have the right to access personal information held by the City request correction if the data is inaccurate, incomplete or out of date. Access to someone's own personal information can be made by contacting the City at governance@fremantle.wa.gov.au. This request will then be considered by the City's Privacy Officer in accordance with both the *Privacy and Responsible Sharing Act 2024 and the Freedom of Information Act 1992*.

5.2. Access to another person's personal information can be made through the City's FOI process by contacting FOI@fremantle.wa.gov.au. This request will then be considered in accordance with both the *Privacy and Responsible Sharing Act 2024 and the Freedom of Information Act 1992*, and this policy where relevant.

5.3. Access to information that does not relate to personal information can be requested via info@fremantle.wa.gov.au or the online service request portal.

6. Automated decision-making

6.1. Where an automated decision-making process using personal information is employed, the City will comply with the PRIS legislation and the Information Privacy Principle: Automated decision-making.

6.2. Where a significant decision is made, the City requires human intervention.

7. Anonymity

7.1. An individual may de-identify themselves when engaging with the City, unless required by law or to do so is impracticable in relation to the matter.

7.2. The City will assist the individual to the best of its ability, but anonymity may limit the outcome of the City's service to or for the individual.

8. Complaints and General Requests

8.1. Complaints in relation to breaches of the *Privacy and Responsible Information Sharing Act 2024* Legislation and this Policy can be lodged with the City by email at governance@fremantle.wa.gov.au.

8.2. Requests and queries relating to this policy can be made to governance@fremantle.wa.gov.au.

9. Third party supplier requirements

9.1. Third party suppliers of the City of Fremantle are to provide a collection notice when collecting personal information to perform functions on behalf of the City.

9.2. Third party suppliers of the City of Fremantle must only use personal information provided by the City for the primary purpose of what it was provided for.

9.3. Third party suppliers are to provide notice to the City of Fremantle if a breach of the personal information collected on behalf of the City or provided to the contactor by the City is identified.

Definitions and abbreviations

"Automated decision-making process" is a process under which a decision is made by an automated system without the involvement of any individual, or the making of decision is materially assisted by an automated system.

a "***significant decision",*** in relation to automated decision-making processes, is one which affects an individual's rights, entitlements, interests or liabilities; or otherwise has a significant effect on an individual's life circumstances, opportunities, behaviour or wellbeing.

"Business purposes" means for purposes associated with the day-to-day business of the City of Fremantle.

"Information breach" means unauthorised access to, or unauthorised disclosure of, information or loss of information.

"Information Privacy Principles" means the information privacy principles (IPP) provided in schedule 1 of the PRIS Act.

"PRIS Act" means the *Privacy and Responsible Information Sharing Act 2024*

"Third Party Supplier" is a contractor, consultant, supplier, or similar that has been engaged by the City to undertake activities on behalf of the City of Fremantle.

"Personal information" means information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion.

This includes information of the following kinds:

- a name, date of birth or address
- a unique identifier, online identifier or pseudonym
- contact information
- information that relates to an individual's location
- technical or behavioural information in relation to an individual's activities, preferences or identity
- inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information
- information that relates to one or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual.

Sensitive personal information includes information that relates to the individual's:

- racial or ethnic origin
- gender identity
- sexual orientation or practices
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- criminal record
  or
- that is health information
- genetic or genomic information
- biometric information.

Responsibility and review information	
Responsible officer:	Manager Governance
Document adoption/approval details	24 June 2026 – Ordinary Meeting of Council – ARIC2606-2
Document amendment details	
Next review date	24 June 2030

Schedule 1 - Information Privacy Principles

1. Collection

An IPP entity must not collect unnecessary personal information. Any personal information collected must be necessary for the functions or activities of the IPP entity.

An IPP entity must collect personal information fairly and reasonably. This includes considering the amount of information collected, its sensitivity, whether an individual would expect it to be collected and any harm or loss to any individual because of the collection.

An IPP entity must not collect personal information in an unreasonably intrusive way.

An IPP entity must only collect sensitive personal information in certain circumstances, for example when required by law or if an individual consents to the collection.

Before personal information is collected, an IPP entity must document why it is being collected and how it will be used or disclosed.

When an IPP entity collects personal information from an individual, it must tell them the reason for its collection, and its use or disclosure, how the IPP entity can be contacted, amongst other details. This information must be clear, concise and up to date.

2. Use and disclosure

An IPP entity must only use and disclose personal information for the reason it was collected. This is called the primary purpose.

An IPP entity may only use or disclose personal information for another purpose in certain circumstances. This is called the secondary purpose.

The circumstances where an IPP entity may use or disclose personal information for a secondary purpose include if an individual consents, the law allows it, to prevent a serious threat of harm to an individual or the public, or if it is necessary for law enforcement or court proceedings.

An IPP entity must use or disclose personal information fairly and reasonably. This includes considering the amount of information used or disclosed, its sensitivity, whether an individual would expect it to be used or disclosed, and any harm or loss to any individual because of the use or disclosure.

Before personal information is used or disclosed for a secondary purpose, an IPP entity must document that purpose.

3. Information quality

An IPP entity must take reasonable steps to make sure the personal information collected, used or disclosed is correct, complete, and up to date.

4. Information security

An IPP entity must take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification, or disclosure.

An IPP entity must take reasonable steps to destroy, or permanently de-identify personal information when it is no longer needed, unless a law requires the IPP entity to keep it.

5. Openness and transparency

An IPP entity must have a publicly available privacy policy that sets out what personal information it collects and holds, and how and why it handles personal information. The privacy policy must also include whether any personal information is used in automated decision-making. Importantly, the policy must be up-to-date, clear, concise and expressed in plain language.

6. Access and correction

An individual can request access to personal information that an IPP entity holds about them. An individual can also request an IPP entity correct the personal information it holds about them if it is not accurate, complete or up to date.

An IPP entity must make a decision about the request for access or correction as soon as practicable, but no later than 45 days after the request was made. If the IPP entity refuses to give access or correct the personal information, it must give an individual valid reasons.

Note: IPP 6 applies only to IPP entities who are contracted service providers to government. Refer to the information below about the exceptions to the IPPs.

The right to access or correct personal information in government documents held by IPP entities that are not contracted service providers is under the Freedom of Information Act 1992 (WA).

No wrong door: If an individual applies to an IPP entity for access or correction of their personal information under the PRIS Act when their right of access is under the FOI Act, or an individual applies under the FOI Act when their right of access is under the PRIS Act, both the FOI Act and the PRIS Act provide that the application should be taken as an application under the correct legislation.

7. Unique identifiers

An IPP entity must not assign a unique identifier to an individual unless it is necessary to perform its functions or activities efficiently.

An IPP entity can only adopt, use or disclose a unique identifier used by another IPP entity for an individual in limited circumstances.

An IPP entity can only require an individual to provide a unique identifier to obtain a service in limited circumstances.

8. Anonymity

An IPP entity must give an individual the opportunity to not identify themself.

An IPP entity can only require an individual to identify themself if the law or circumstances make it necessary.

9. Disclosures outside Australia

An IPP entity must not send personal information overseas unless certain requirements are met. This includes, for example, that the overseas recipient of the information is subject to similar requirements as the IPP entity under the IPPs.

Further, an IPP entity must not send de-identified information overseas unless the recipient has appropriate security in place to protect the information and does not try to re-identify it.

10. Automated decision-making

If an IPP entity makes important decisions about individuals using automated decision-making processes (that is a process without much human input), it must assess the risks to ensure harm, bias and discrimination is minimised and that the requirements of the PRIS Act are complied with. This should be done periodically and when changes are made to the automated decision-making.

An IPP entity must let individuals know it is using automated decision-making and there must be a process where people can request human involvement in the decision.

11. De-identified information

An IPP entity must take reasonable steps to protect the de-identified information it holds from misuse, loss, unauthorised re-identification, access, modification or disclosure.

An IPP entity must not re-identify de-identified information unless certain circumstances apply.