



1/031 Privacy Policy

Objective

The objective of this policy is to state the Town of Port Hedland's (the Town) commitment to protect the privacy of all persons associated with the Town when collecting, using, disclosing, and managing personal information.

This commitment will achieve compliance with the State Privacy and Responsible Sharing (PRIS) Act 2024 and its Information Privacy Principles (IPPs).

Content

Scope

The Town of Port Hedland, its Councillors, Employees and Contractors collect handle, store and share personal information from internal and external stakeholders as part of their regular business activities. The Town will take reasonable steps to protect the information from misuse, interference, and loss, as well as unauthorised access, modification or disclosure.

Principles

The Town is required to collect and manage personal information for business purposes only and therefore must consider the risks involved in details of, or copies of, personal information and must take steps to manage that information appropriately and in accordance with the following information privacy principles.

Principle 1: Personal information and why it is collected.

Personal information is information or an opinion that identifies an individual. Examples of personal information the Town collects include names, addresses, email addresses and phone numbers.

The Town collects personal information for the primary purpose of providing services to the Port Hedland community. Personal information may also be used for secondary purposes closely related to the primary purpose, in circumstances where it is reasonable to do so.

The Town will not collect personal information, including sensitive personal information, unless it is necessary for Town business functions and activities and legal purposes.

The Town will only collect personal information with a person's consent for that collection unless it is not practical to seek that consent.

The Town will ensure personal information is up-to-date, clear and concise.

Principle 2: Use and disclosure

When the Town collects personal information the owner of that information will be informed of the reason for collecting their information and how it will be used.

When personal information is collected it will be used only:



- for the primary purpose for which it was collected; or
- for a secondary purpose that is directly related to the primary purpose; or
- with the owner's consent; or
- where required or authorised by law; or
- where there is a serious threat to the life, health, safety or welfare of an individual; or
- where illegal activity may have occurred

The Town will not use or disclose personal information unless it has considered the kind and amount of information, if it is necessary for business functions and activities, the risk of loss or harm, if it is in the public interest, if it is in the best interests of a child and if it meets the objectives of the Privacy and Information Sharing Act 2024.

A written record will be kept where personal information was collected for a primary purpose and has been used for a secondary purpose or disclosure.

Principle 3: Information Quality

It is important that personal information is correct. The Town will take reasonable steps to ensure that personal information is accurate, complete and up to date. When contacted by the owner of the information, the Town will update its records of personal information held, that is not correct, to ensure quality services.

Principle 4: Information security

Personal information will be stored in a manner that protects it from misuse and loss and from unauthorized access, modification, or disclosure.

When personal information is no longer needed for the purpose for which it was obtained, the Town will dispose of that information in accordance with the General Disposal Authority for Local Government.

The Town will retain and dispose of all records, including personal information, in accordance with the approved General Disposal Authority for Local Government. When destroying any records, especially those containing personal and sensitive information, the Town will ensure it is done completely so that no information is retrievable.

Principle 5: Openness and transparency

This policy will be publicly available to ensure the community is aware of how personal information is collected and managed by the Town of Port Hedland.

These documents will be maintained and kept current as regulations and the types of personal information collected may change.

Principle 6: Access and correction

The Town's privacy management plan will outline key roles and responsibilities for privacy management. Internal access to personal information will be limited to only those roles / individuals who need access for business purposes. This applies to hardcopy files and having access permissions embedded in systems which manage records.



A person may access the personal information the Town holds about them to update and/or correct it, subject to IPP 6.1 of the PRIS Act. To access personal information, a request must be made to the Town in writing. The Town will not charge any fee for access requests but may charge an administrative fee for providing a copy of personal information. In order to protect personal information, the town may require identification from an individual before releasing the requested information.

Principle 7: Unique identifiers

Individuals engaging with the Town will not be assigned unique identifiers unless they are required to perform business activities efficiently.

Any identifiers assigned will not be those from another organisation or be used by or disclosed to any other organisation.

Some circumstances may require the town to use or obtain unique identifiers such as when it was obtained for a directly related purpose, when the individual gives consent, when required by law, for suspected unlawful activity, for research or legal proceedings.

Principle 8: Anonymity

When doing business, engaging, or communicating with the Town people will not be required to identify themselves unless required to under the law or it is not practical for the Town to provide service without the person's identity.

Principle 9: Disclosures outside Australia

The Town will not disclose anyone's personal information, including de-identified information, outside Australia unless it is lawful, the recipient of the information operates under law which makes them compliant with these principles, with the individual's consent, forms part of a contract, or for the benefit of the individual.

Principle 10: De-identified information

The Town will protect any de-identified information received and held from re-identification, access, modification, or disclosure.

The Town is committed to recording, using, storing, and destroying all personal and sensitive information with respect and in accordance with written laws and these principles.



Definitions

“Agency” means a Minister or a public body or office and the agency to which an access application for amendment of personal information has been made or to which such an application has been transferred or partly transferred.

“Business Activities” major tasks performed by the Town as part of its responsibilities for achieving the strategic goals of the Town on behalf of the Community.

“Collect” in relation to information:

- a) means to obtain the information from any source or by any means; and
- b) includes information from, or generated by, the use or interpretation of other information.

“Consent” means express consent or implied consent.

“De-identify” personal information means to modify, or apply a process to, the information, with the result that the identity of an individual is not apparent, and cannot reasonably be ascertained, from the information.

“Disclose” information:

- (a) includes a reference to the Town making the information publicly available; and
- (b) does not include a reference to the Town disclosing the information to itself or to an officer of the Town.

“Information Privacy” includes the right of a person to be able to control who can see or use information about them.

“Personal Information” 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 and includes:

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

“Re-identify” de-identified information means to modify, or 1 apply a process to, the information, with the result that the 2 information again becomes personal information.



“Sensitive Information” a subset of personal information meaning information or an opinion about an individual’s race or ethnic origin, political opinions, membership of a political association, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, gender identity, sexual practices, criminal record and health information.

Relevant legislation	<ul style="list-style-type: none"> ▪ Privacy and Responsible Information Sharing Act 2024 ▪ Freedom of Information Act 1992 ▪ State Records Act 2000.
Relevant Standards	<ul style="list-style-type: none"> ▪ Information Privacy Principles ▪ General Disposal Authority for Local Government ▪ State Records Office of Western Australia State Records Commission Standards and Advice
Delegated authority	Senior Records Officer
Business unit	IT & Program Delivery
Directorate	Corporate Services

Supporting Documents

- Privacy Management Plan
- Privacy Complaints Procedure
- Data Sharing Request Procedure
- Privacy Impact Assessment Procedure

Related Documents

- Records Management Policy
- Information Classification Policy
- Information Management Policy
- Data Breach Policy



Governance to complete this section			
Version Control	Version No.	Resolution No.	Adoption date
	Version 1.0	CM202425/192	27 November 2024
Review frequency	Annually		

Document Control Statement – The electronic reference copy of this Policy is maintained by the Governance Team. Any printed copy may not be up to date and you are advised to check the electronic copy at <http://www.porthedland.wa.gov.au/documents/public-documents/policies> to ensure that you have the current version. Alternatively, you may contact the Governance Team.