COUNCIL POLICY

Information Privacy

Policy Objective

This Policy, aligns with the *Privacy Act 1988,* and complies with the *Privacy and Responsible Information Sharing Act 2024* which mandates how government agencies can protect personal information of members of the public and Shire Employees, ensuring transparency and providing clear guidelines on when, how, and to what extent their information is collected, used, and managed.

Policy Scope

This policy applies to all employees, contractors, elected members and agents of the Shire of Broome who handle personal information in the course of their duties.

Policy Statement

The Shire of Broome is committed to protecting the privacy of individuals, which we acknowledge as a fundamental human right.

Definitions:

- **Information Privacy**: refers to People's personal and sensitive information and their right to control when, how and to what extent it is used.
- **Personal Information:** any information that can identify an individual, such as name, address, phone number, email address, and other identifying details.
- **Sensitive Information:** information that includes racial or ethnic origin, political opinions, religious beliefs, health information, and other sensitive data.
- **Collection Notice:** a notice provided when personal information is collected that explains why the information is being collected, how it will be used and disclosed, and the individual's privacy rights under the *Privacy and Responsible Information Sharing Act 2024 (WA).*
- **Information Classification:** a business-level process whereby the sensitivity of a piece of information is evaluated, and a classification label applied to it, such that the sensitivity will be clear to all those who subsequently access it. (see the WA Government Information Classification Policy 2020).
- **Information Asset Register:** a comprehensive list of types of information and the systems that store the information or produce the information themselves – anywhere we store information that is critical to the running of our agency.

- **Responsible Information Sharing:** the sharing of information in a manner that is lawful, necessary, proportionate and consistent with the requirements of the *Privacy and Responsible Information Sharing Act 2024 (WA).*

- **Privacy Breach:** means unauthorised access, disclosure, loss or misuse of personal information.

Governing Legislation

- *Privacy and Responsible Information Sharing Act 2024 (PRIS Act)*
- *The Information Privacy Principles (IPPs)*
- *Privacy Act 1988*
- *State Records Act 2000*
- *Freedom of Information Act 1992*
- *Information Commissioner Act 2024*
- *Local Government Act 1995*

Management Guidelines

Information Privacy Principles (IPPs):

The Information Privacy Principles (IPPs) are set out in Schedule 1 of the *Privacy and Responsible Information Sharing Act 2024 (WA)*

- **IPP 1:** Collection – Fair, necessary, and documented collection of personal information.
- **IPP 2:** Use and Disclosure – Limitations restricting use and disclosure to primary or secondary purposes.
- **IPP 3:** Quality – Requirements to keep personal information accurate and up-to-date.
- **IPP 4:** Security and Destruction – Obligations to protect information and securely destroy or de-identify it.
- **IPP 5:** Openness – Transparency through clear privacy policies.
- **IPP 6:** Access and Correction – Rights for individuals to access and correct their information (with a 45-day response window).
- **IPP 7:** Unique Identifiers – Restrictions on the use and adoption of unique identifiers.
- **IPP 8:** Anonymity – Providing individuals the option to remain anonymous or not identify themselves where practicable.
- **IPP 9:** Disclosures Outside Australia – Rules ensuring equivalent protection when transferring data overseas.
- **IPP 10:** Automated Decision-Making – Mandating transparency, procedural fairness, and privacy impact assessments for automated decisions.
- **IPP 11:** De-identified Information – Protections and re-identification limits regarding de-identified data

Collection Notices

The Shire of Broome will take reasonable steps to ensure that individuals are informed whenever personal information is collected directly from them.

Where practicable, collection notices will be provided at or before the time personal information is collected and will include:

- the identity and contact details of the Shire;
- the purpose(s) for which the information is being collected;
- whether the collection is required or authorised by law;
- the consequences, if any, of not providing the requested information;
- how the information may be used or disclosed;
- how the individual may access and request correction of their personal information.

Collection notices may be provided through forms, applications, websites, online services, customer service interactions, correspondence, public consultation processes, employment-related processes and any other collection mechanism utilised by the Shire.

Disclosing personal information for a secondary purpose, without consent:

Where the secondary purpose is related to the primary purpose and the Individual would reasonably expect the disclosure.

Where the use or disclosure is necessary for action to be taken against suspected unlawful activity or serious misconduct relating to the agency's functions.

Where the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

Information Classification Plan

The WA Government Information Classification Policy 2020 provides direction for public sector agencies to label their information according to its sensitivity.

It requires all government agencies to:

Clearly and consistently identify sensitive information;
Apply appropriate security measures; and
Communicate the classification within the agency and with others.

The three classifications mandated under the Policy align with the Aust Government protective markings for non-security classified information in its Protective Security Policy Framework.

UNOFFICIAL
OFFICIAL
OFFICIAL: Sensitive

This is primarily a risk management activity. Information classification is the responsibility of the entire business, NOT a delegated task for ICT teams.

A Business Operating Procedure for the classification of the Shire's information will mandate how our information will be classified and marked with appropriate classification labels.

Note: Agencies are not required to conduct a classification process on existing information until they are use

Information Asset Register (IAR)

IAR is a critical component of data management and security – particularly in relation to increasing Cyber compromises.

Data management and the development of an IAR is not just the responsibility of Information and Records Management, or ICT, it is important that we can rely on the custodians of the systems and the information they hold to ensure that we have a comprehensive IAR.

An IAR should be a body of information, defined and practically managed so that the Information and systems can be understood, shared, protected and used to their full potential. An IAR should have:

- **A set of guiding principles incorporated into process documents**.
- A process for the creation, maintenance, use of, and reporting of an IAR, including destruction principles.
- Clearly identified vital records – critical to business requirements.
- Information of historical value and Corporate legacy.
- Documents with a legal or regulatory obligation.
- Documents with protective classification – sensitive and confidential.
- And IT component identified, classified and managed – integration with IT is essential

A Business Operating Procedure for the process for developing and maintaining the Shire's Information Asset Register will mandate how the register is used and who is responsible for the collecting of information and maintenance of the register.

Responsible Information Sharing

The Shire may share information with authorised entities where permitted by law and where the sharing:

- supports lawful functions or public benefit outcomes;
- is proportionate and necessary;
- appropriately manages privacy risks;
- complies with approved information sharing arrangements; and
- is adequately documented and auditable.

Privacy Breach Management

The Shire will establish and maintain procedures for identifying, assessing, responding to and reporting eligible privacy breaches in accordance with the Privacy and Responsible Information Sharing Act 2024 (PRIS Act) and associated regulations.

Compromised can mean any of the following:

- Physical unauthorised access.

- Phishing – scam emails, SMS to trick people into providing sensitive information, or clicking on malicious links or attachments.
- Drive-by – when attackers hack into a legitimate site and install malware that will infect anyone who visits the site.
- Watering-hole – targeted attacks that take advantage of your interests to strategically infect many people in certain groups.
- USB devices – when attackers infect USB devices using malicious software that will run automatically when plugged in.

Note: Security breaches are not always Criminal Acts – they can be accidental such as leaked documents, unprotected data, information sent to wrong person.

Review and Improvement

Once the breach has been addressed, the Incident will be reviewed by key stakeholders including, the Director Corporate Services, the Manager Governance, Risk and Strategy and the Manager Information Services to identify any weaknesses in privacy practices and processes. An improvement plan will then be recorded and presented to the CEO and the Executive Management Team.

Roles & Responsibilities

Director Corporate Services

Will ensure there is published to the Shire Website, and also to the Intranet, a clearly expressed, up-to-date privacy policy. As the PRIS Champion the Director will oversee compliance, provide guidance, and manage risks related to the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act).

Manager Information Services

Will take reasonable steps (in compliance with relevant Policies and Cyber security and protection procedures) to ensure that the personal information collected is protected from Misuse, loss or interference:

1. Unauthorised access; and
2. Disclosure (other than intended purpose).

Records Services Coordinator

Will develop and maintain an Information Asset Register which forms part of the Shire's Information Classification Implementation Plan. As the Privacy Officer under the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) the Records Coordinator will promote compliance with the IPPs and PRIS privacy provisions, coordinate the preparation of the information breach policy, maintain the register of notifiable information breaches, and coordinate responses to privacy complaints.

All Employees

Shire Employees dealing with members of the public, and/or involved with the collection and storing of personal information about individual members of the public will follow the basic IP principles, in particular:

1. Informing the public on why we are collecting information, what we will do with it and who might see it,
2. Only collecting information that is essential to the functions performed by the Shire;
3. Using information provided only for the original intended purpose;
4. Taking reasonable steps to ensure that the information we collect, use and share is accurate and legible;
5. Storing personal information securely, protected from unauthorised access, and destroyed in a timely manner in accordance with the GRDALG 2023-005; and
6. Using empathetic and open communication and consultation handle requests and complaints with care and diligence and assist Customers to see their own personal information and change it where applicable.
7. Report Privacy Breaches immediately.

Document Control Box			
Document Responsibilities:			
Owner:	Director Corporate Services	**Owner Business Unit:**	Information Services
Reviewer:	Manager Information Services	**Decision Maker:**	Council
Compliance Requirements:			
Legislation:	*The Privacy Act 1988* *Local Government Act 1995* *Privacy and Responsible Information Sharing Act 2024* *State Records Act 2000* *Freedom of Information Act 1992* *WA Information Classification Policy 2020*		
Industry:			
Organisational:	Council Policy Information Services Physical and Environmental Security Council Policy Records Management Record Keeping Plan 2024 Business Operating Procedure Information Asset Register Freedom of Information Admin Policy Information Classification Admin Policy		

Document Management:					
Risk Rating:	**Moderate**	**Review Frequency**:	**Biennial**	**Next Due:**	**2/2028**

Version #	**Decision Reference:**	**Synopsis:**
1.	27/02/2025	Initial Adoption by Council – February 2025 OMC Min C/0225/009
2.	28 October 2026	Reviewed. Adopted by Council OMC 28 October 2026 Resolution C/1026/008