COUNCIL POLICY

Information Privacy

Policy Objective

This Policy, aligns with the *Privacy Act 1988,* to 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.
- **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.

Management Guidelines

The Australian Privacy Principles (APPs):

The set of 13 APPs form the cornerstone of the privacy protection framework in the Privacy Act. They apply to any organisation or agency covered by the Privacy Act.

1-2 Planning and Governance

1. Open and Transparent – making available a clearly expressed privacy policy about the management of personal information by the agency.
2. Anonymity & Pseudonymity – individuals have the option of not identifying themselves or making use of a pseudonym where they choose.

3-5 Collection

3. Collecting Personal information - is only collected where it is required for the function of the agency. Information should be collected directly from the person with consent to collect sensitive information.
4. Unsolicited Personal Information – within a reasonable period of time after receiving and determining it was not solicited, the information should be as soon as practicable disposed of.
5. Giving Notice – Individuals must be given notice when are collecting information about them, and why.

6-9 Handling

6. Using or disclosing information – Personal information collected about an individual can only be used for the purpose it was collected; it must not be used or disclosed for a secondary purpose.(see below note1 on when information can be disclosed.)
7. Direct Marketing – Agencies that hold personal information must not use or disclose the information for the purpose of direct marketing unless reasonably expected to or consent is provided by the individual.
8. Cross-border disclosure – before disclosing personal information to an overseas recipient, reasonable steps must be taken to ensure that the overseas recipient doesn't breach the APPs.
9. Adoption, use or disclosure – outlines circumstances when an agency may adopt a government related identifier of individual as its own.

10-11 Integrity

10. Quality of Information – Reasonable steps need to be taken to ensure that the personal information collected is accurate, complete and relevant before it is disclosed or used,
11. Security – Reasonable steps need to be taken to ensure that the personal information is protected from misuse, loss and/or interference, unauthorised access, modification or disclosure. An Agency has the obligation to destroy or de-identify personal information where it is no longer needed, or where the information is not contained in a Commonwealth record required by law to retain.

12-13 Access and Control

12. Access – Individuals must be provided access to the information collected about them unless any exceptions apply. Requests for access must be responded to within a reasonable period of time.
13. Correction of Personal Information – Reasonable steps should be taken to correct personal information and ensure it is relevant, accurate, complete and not misleading.

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.

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.

Manager Governance, Strategy and Risk

Will regularly review and update the Shire of Broome Council Privacy Policy.

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

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 AAP 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.

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.

Document Control Box

Document Responsibilities:			
Owner:	Director Corporate Services	**Owner Business Unit:**	Governance
Reviewer:	Manager Governance, Strategy and Risk	**Decision Maker:**	Council

Compliance Requirements:	
Legislation:	*The Privacy Act 1988* *Local Government Act 1995*
Industry:	State Records Act 2000 Freedom of Information Act 1992 WA Information Classification Policy 2020
Organisational:	Council Policy Information Services Physical and Environmental Security Council Policy Records Management Record Keeping Plan 2024 Business Operating Procedure Information Asset Register

Document Management:						
Risk Rating:		**Review Frequency**:	**Reviewer**	**Annual Desktop**	**Next Due:**	
			Council			

Version #	Decision Reference:	Synopsis:
1.	Initial Adoption	Endorsed by Council at OMC of
2.		
3.		