2.38 PRIVACY AND INFORMATION BREACH POLICY

Responsible Directorate	Corporate Services	
Responsible Service Area	Governance	
Resolution	April 2029	C.2.4.2026
Procedure Ref	N/A	

1. PURPOSE

The Shire of Mundaring (Shire) views privacy compliance as an integral part of its commitment to accountability and integrity. The Shire values the privacy of its customers and stakeholders and is committed to upholding the highest standards of information privacy in alignment with the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act).

The purpose of this Policy is to provide clear and consistent guidelines to support the Shire in handling personal information responsibly, lawfully, and transparently. The Policy will ensure the Shire takes reasonable steps to protect the information it handles from misuse and loss and from unauthorised access, modification, or disclosure.

2. SCOPE

This policy details the types of personal information the Shire collects, what it's used for and how it's stored, and the measures in place to prevent and respond to information breaches.

This policy applies to all Shire employees, Council Members, and individuals engaged to perform work on behalf of the Shire, including:

- contractors and consultants,
- temporary labour and service providers,
- volunteers, and
- third-party providers.

The Shire requires all contracted service providers to comply with this policy.

3. DEFINITIONS

Contracted Service Provider refers to a party to a services contract who provides services to or on behalf of an outsourcing entity under the contract, or a person who is a direct or indirect subcontractor of the party for the purposes of the services contract.

Council Member: a person who is currently serving a term of office as an elected member of the Council in accordance with the *Local Government Act 1995.*

De-identified information means personal data that has been modified or processed in such a way that the identity of an individual is no longer apparent and cannot reasonably be determined from the information.

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

Information Sharing Agreement refers to the agreement or mechanism between entities to share information under the PRIS Act.

Personal Information means personal information as defined in section 4 of the PRIS Act.

Sensitive Personal Information means sensitive personal information as defined in section 4 of the PRIS Act.

4. POLICY POSITION

The Shire takes reasonable steps to protect personal information by preventing misuse, loss, unauthorised access, re-identification, modification, or unauthorised disclosure.

5. POLICY

5.1. Collection

The Shire collects personal information only when necessary to fulfil its functions, meet statutory obligations, deliver services, and support day-to-day operations. This includes, but is not limited to, the following:

5.1.1. Email, written, online and in person requests, applications, submissions, complaints, feedback and general enquiries related to the delivery of Shire services.

5.1.2. Employment details during recruitment, onboarding and throughout employment.

5.1.3. Video or audio call recordings for monitoring responses, training and quality assurance.

5.1.4. Data from third-party platforms and cloud services supporting Shire operations.

5.1.5. CCTV footage for safety, security, and operational purposes in public spaces.

5.1.6. Location data and device identifiers, from Shire-approved websites and mobile apps.

5.1.7. Community surveys, including details voluntarily provided for planning and policy development.

5.1.8. Website analytics and cookies, including on the Shire's digital platforms to personalise content and improve user experience.

5.1.9. Procurement details, including the collection of information from suppliers and contractors through the Shire's procurement systems.

5.1.10. Inter-agency collaboration details, to support the delivery of joint initiatives.

5.2. Conditions of Collection

The Shire will only collect personal information when:

5.2.1. it is necessary for the Shire's core functions (primary purpose),

5.2.2. it relates to other Shire functions that the individual would reasonably expect (secondary purpose),

5.2.3. it is authorised by law,

5.2.4. the individual has provided consent, or

5.2.5. it is required for research conducted in the public interest.

5.3. Use and Disclosure

The Shire uses personal information for the purpose for which it was collected. The Shire may also use information for another purpose when:

5.3.1. the person would reasonably expect this use (secondary purpose),

5.3.2. the person has given consent,

5.3.3. the law requires or permits it,

5.3.4. it is needed to prevent serious harm or protect safety,

5.3.5. it is needed to investigate unlawful activity,

5.3.6. it is needed to develop, maintain or improve our services, technology or customer experience, or

5.3.7. it is needed for research in the public interest, where people cannot be identified and it is not practical to get consent.

The Shire will not disclose personal information to third parties without the individual's consent, unless:

5.3.8. the person would reasonably expect the disclosure because it is related (or, if sensitive, directly related) to the reason the information was originally collected, or

5.3.9. the disclosure is with an organisation or government agency that funds or arranges services for the individual, or

5.3.10. it is required or permitted by law,

5.3.11. it is necessary to address an imminent and serious risk to an individual's life, health, or safety, or

5.3.12. it is in accordance with a formalised Information Sharing Agreement.

To support its operations and service delivery, the Shire may share personal information with contracted service providers or other government entities, for the purpose of:

5.3.13. conducting community consultation or research,

5.3.14. delivering goods, infrastructure, or services, or collaborating with other government entities, including local, state, or federal agencies, where required to deliver services or where an Information Sharing Agreement is in place.

When sharing or accessing data with third parties, the Shire must comply with the conditions in any agreements, licences, or memoranda of understanding. These agreements govern how State and Federal agencies, including WA Police, use and access specific data resources.

Where a contracted service provider stores personal information, the Shire requires that party to comply with this policy.

5.4. Information Quality

The Shire cannot guarantee that the personal information it holds is accurate, for reasons including errors, omissions, and information becoming outdated over time.

However, the Shire will take all reasonable steps, as appropriate in the circumstances, to ensure accuracy and completeness of personal information upon collection or before it is shared.

5.5. Information Security

Personal information is stored in on-premises and cloud-based systems.

Where cloud services are used, they are hosted in Australia and must comply with Australian privacy laws and contracted information security requirements.

Controls will be implemented to protect the information the Shire holds, including:

5.5.1. multi-factor authentication;

5.5.2. access controls;

5.5.3. endpoint detection and response (EDR);

5.5.4. encryption of data at rest and in transit;

5.5.5. regular security patching and vulnerability management;

5.5.6. a managed Security Information and Event Management (SIEM) service; and

5.5.7. ongoing cybersecurity awareness training for staff.

The Shire will ensure that personal information is not kept any longer than necessary or destroyed or de identified in line with accepted document disposal schedules and the Shire's Recordkeeping Plan.

5.6. Access and Correction

Individuals have the right to request access to their personal information held by the Shire and to seek correction if the information is inaccurate, incomplete, or out of date.

All requests will be managed in accordance with the Shire of Mundaring Customer Service Charter.

Requests to access or correct personal information held by the Shire must be submitted in writing to:

Chief Executive Officer

Shire of Mundaring

7000 Great Eastern Highway

Mundaring WA 6073

Or via email to: shire@mundaring.wa.gov.au

Where access to personal information is sought, individuals may be required to submit a formal Freedom of Information (FOI) request. Where access is refused, the Shire will provide written reasons and inform the individual of their right to seek review.

5.7. Unique Identifiers

Unique identifiers (such as driver's licence numbers) will only be collected if it is:

5.7.1. necessary to carry out the Shire's official functions, or

5.7.2. required by law.

When unique identifiers are collected, the Shire ensures they are handled securely and used only for their intended purpose.

5.8. Anonymity

Where it is lawful and practical, the Shire of Mundaring will give individuals the option to remain anonymous or use a pseudonym when interacting with the Shire.

This may apply to general enquiries, feedback, or participation in surveys where personal identification is not required.

In some cases, providing personal information may be necessary to deliver services or respond to specific requests.

5.9. Automated Decision Making

The Shire may use automated decision-making to support minor decisions involving personal information to streamline services and enhance the customer experience, such as during the review of application assessments or routing of customer queries and requests.

Automated decision-making does not replace human decision-making for significant or high-risk decisions.

5.10. Disposal & De-identification

The Shire will securely and permanently destroy or de-identify personal information when it is no longer needed by law.

Disposal is conducted in a manner that ensures complete destruction of personal information, making it irretrievable.

5.10.1. Protection of de-identified information

The Shire will document all de-identification processes and ensure that de-identified data is handled securely.

Digital records are de-identified appropriately before disposal, such as when decommissioning devices or systems.

5.10.2. Retention of Documents

Copies of proof-of-identity documents will not be retained unless required. Instead, a record of sighting will be created.

Unsolicited copies will be destroyed immediately.

5.11. Information Breaches

The Shire will conduct regular security assessments to detect and prevent data misuse or loss. If an information breach occurs, the Shire will investigate the extent of the incident and ensure appropriate containment and mitigation measures are applied.

5.11.1. Employee Responsibilities

The Shire requires all employees to immediately report any actual or suspected privacy breach, cyber incident, unauthorised access, disclosure, or loss of personal information to the Privacy Officer.

5.11.2. Mandatory Reporting

The Shire will comply with mandatory information breach reporting requirements when they commence under the PRIS Act. Where applicable, the Shire will notify the WA Information Commissioner and relevant law enforcement agencies.

5.11.3. Information Breach Prevention

The Shire will take proactive steps to reduce the risk of information breaches, including:

5.11.3.1. Ongoing monitoring of systems,

5.11.3.2. Regular security assessments,

5.11.3.3. Maintaining effective information security controls, and

5.11.3.4. Providing regular privacy and security training for staff.

5.11.4. Information Breach Response Process

If a breach occurs, the Shire will follow its Information Breach Response Plan by:

5.11.4.1. Containing the breach,

5.11.4.2. assessing the impact,

5.11.4.3. notifying affected parties (if required), and

5.11.4.4. preventing future occurrences.

The Privacy Officer is responsible for determining whether notification is required and identifying who needs to be notified.

All information breaches will be recorded in the Shire's Information Breach Register. Information recorded includes:

5.11.4.5. The type of breach (e.g. unauthorised access, disclosure, or loss),

5.11.4.6. Whether personal information was affected,

5.11.4.7. Assessment outcomes (if the breach meets the notifiable definition),

5.11.4.8. Details of who was notified and when (e.g. affected individuals or the Information Commissioner),

5.11.4.9. Actions taken to reduce harm and prevent recurrence, and

5.11.4.10. The estimated impact or cost of the breach.

5.12. Complaints

Complaints of alleged interferences with personal information may be made to the Shire. This may include unauthorised access, loss or disclosure of personal or sensitive personal information.

All complaints will be managed in accordance with the Shire of Mundaring Customer Service Charter. Complaints must be submitted in writing to:

Chief Executive Officer

Shire of Mundaring

7000 Great Eastern Highway

Mundaring WA 6073

Or via email to: shire@mundaring.wa.gov.au