Council Policy – Privacy and Information Handling

Responsible Directorate	Office of the Chief Executive Officer
Responsible Business Unit/s	Information and Communications Technology (ICT)
Responsible Officer	Manager ICT
Affected Business Unit/s	All

Objective

This policy details how the Shire of Ashburton (Shire) manages the collection, storage and use of personal information to ensure privacy risks are appropriately managed.

Scope

This policy applies to all elected members, employees, contractors and volunteers undertaking duties on behalf of the Shire. It extends to all information handled by the Shire, including, information regarding customers, stakeholders, employees, contractors, volunteers, elected members and committee members.

Policy Statement

The Shire values the privacy of its customers and stakeholders and takes reasonable steps to protect the information it handles from misuse and loss, and from unauthorised access, modification, or disclosure. The Shire is committed to full compliance with the obligations and requirements of the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act).

Information Handling

Collection of personal information

The Shire collects personal information about its customers and stakeholders in the performance of its functions and activities. Sensitive personal information is not collected, unless:

- it is necessary for the performance of one or more of the Shire's statutory functions and its activities to support the community; and
- the individual consents to the collection; or
- it is required or authorised by or under law; or
- it is necessary for the establishment, exercise or defence of a legal or equitable claim; or

- it is necessary for research, or the compilation or analysis of statistics, relevant to government-funded targeted welfare or educational services; or
- if the use or disclosure is necessary to prevent or lessen:
    - a serious threat to the life, health, safety or welfare of any individual; or
    - a serious threat to public health, public safety or public welfare; or
    - a threat to the life, health, safety or welfare of any individual due to family violence.

Access and correction of personal information

Under the Freedom of Information process a person has rights to access, correct and protect their personal information. Access to someone's own information can be made by contacting the Shire at soa@ashburton.wa.gov.au. This request will then be considered by the Shire's Privacy Officer in accordance with both the *Privacy and Responsible Sharing Act 2024* and the *Freedom of Information Act 1992*.

Visit the Shire's Freedom of Information webpage for further information.

Disclosure of information to third parties

The Shire may disclose customer and stakeholder information to third parties in the following circumstances:

- Under an information sharing agreement or information sharing request, with another public entity;
- With the consent of the customer or stakeholder;
- Where the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
- As required or authorised by law or in response to a request from an investigative authority;
- If the use or disclosure is necessary for a law enforcement function to be performed by a law enforcement agency;
- To complete the purpose or function for which the information was provided;
- To improve the purpose or function for which the information was provided;
- If the use or disclosure is necessary to prevent or lessen:
    - a serious threat to the life, health, safety or welfare of any individual; or
    - a serious threat to public health, public safety or public welfare; or
    - a threat to the life, health, safety or welfare of any individual due to family violence.
- If it believes on reasonable grounds that non-compliance with the proposed PRIS legislation is necessary for the purposes of its, or any other entity's, child protection functions; and/or

- If the information relates to family violence or alleged family violence and the individual to whom the collected information relates is the perpetrator, or alleged perpetrator, of the family violence.

Protection of information

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

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

Multiple controls are implemented to protect information including encryption, multifactor authentication, security awareness training campaigns, endpoint security, email security, domain security, network security, third party risk assessments and other recommended controls defined in the Australian Signals Directorate Essential Eight Maturity Level One.

Privacy and Information Breaches

Responding to interferences with privacy

Complaints regarding acts or practices of the Shire that may constitute an interference with the privacy of an individual can be lodged with the Shire's Privacy Officer by email soa@ashburton.wa.gov.au or telephone on (08) 9188 4444.

The Privacy Officer will aim to provide the complainant with a formal response as soon as practicable, upon receiving all required information. Complainants will be advised of any unavoidable delay.

Interference with the privacy of an individual/s may also amount to an information breach. Information breaches include unauthorised access to, or unauthorised disclosure of information or loss of information.

In the event of an alleged interference with privacy, a person may complain to the Western Australian Information Commissioner. It is the duty of the Information Commissioner, and members of Commissioner staff, to assist an individual who wishes to make a privacy complaint and requires assistance to formulate the complaint.

Responding to information breaches

All complaints made are treated seriously and in accordance with the PRIS Act. The table below sets out the process of responding to information breaches.

Reporting	Incidents related to information breaches must be reported immediately to the Shire's Privacy Officer via email at soa@ashburton.wa.gov.au. Any breach that relates to suspected misconduct is to be reported in accordance with the Shire's Employee Code of Conduct and/or the Code of Conduct for Council Members, Committee Members and Candidates.

Contain	All Shire officers must take reasonable steps to contain the suspected notifiable information breach. This obligation is ongoing as other steps proceed.
Initial Assessment	Within 2 business days, the Shire will make an initial assessment as to whether there is reasonable suspicion that a notifiable breach has occurred. If so, the Shire will notify the affected people and regulator as soon as possible and commence a formal assessment.
Assessment	Within 30 days, determine whether or not a notifiable information breach has occurred or there are reasonable grounds to believe it has occurred and prepare a written report on the assessment.
Notification	Notification to the Western Australian Information Commissioner must be made as soon as possible after the assessment. For assessed shared agency breaches, notification must also be sent to the Chief Data Officer of Western Australia. The Shire will take all reasonable steps to give written notice of an assessed notifiable information breach to each affected individual or publish a written notice of the breach.
Post-Incident Review	A post incident review will consider: • All reasonable steps to mitigate any harm caused by the notifiable information breach; • The steps to be taken to prevent similar future breaches or mitigate the identified risk; • A cause analysis of the breach; • Security audit of both physical, technical and cyber security controls; • Review of employee training practices; • Review of contractual obligations with contracted service providers; and • Any other review considerations, recommendations or guidelines published by the Western Australian Information Commissioner or the Chief Data Officer of Western Australia.

Roles and responsibilities

The below sets out the roles and responsibilities of key stakeholders of the Shire regarding information breaches.

All employees, contractors, volunteers and elected members	• Ensuring that they are familiar with Shire's PRIS obligations and how they apply to their work. • Immediately reporting or referring information breaches or identified privacy risks.
Data Breach Crisis Management Team	• This team is enacted in accordance with the Shire's Data Breach Handling Procedure and is responsible for containing, remediating and recovering the services after an incident.
Privacy Officer	• Promotes the Shire's compliance with the Information Privacy Principles ('IPP'). • Assists in the conduct of privacy impact assessments by the Shire. • Coordinates the preparation of the Shire's response to complaints regarding acts or practices of the Shire that may constitute an interference with the privacy of an individual including privacy interferences that may constitute an information breach. • Coordinates the Shire's dealings with the Western Australian Information Commissioner. • Refers any information breaches that relate to suspected employee or elected member misconduct to the Shire's Chief Executive Officer.

Information Sharing Officer	• Coordinates the Shire's dealings with the Chief Data Officer of Western Australia.
	• Coordinates information sharing requests made by, or to, the Shire.
	• Coordinates information sharing agreements entered into or proposed to be entered into by the Shire and presents such agreements to the Chief Executive Officer for consideration.
	• Assists in the conduct of the following:
	  ○ Assessments of the responsible sharing principles.
	  ○ Privacy impact assessments.
	  ○ Aboriginal information assessments.

Audit, Risk and Improvement Committee	• Maintains oversight of artificial intelligence risks and any information breaches through reporting.
Crisis Management Team (ELT)	• Foster a culture and values that ensures privacy is embedded in the work environment. • Ensure that any privacy impact associated with new initiatives is assessed and steps are taken to mitigate privacy risks. • Advise senior management of information breach incidents.
External Reporting	• People may contact the Western Australian Information Commissioner regarding interferences with privacy and information breaches. • People may contact the Chief Data Officer of WA regarding shared information breaches.

Definitions

Data Breach Crisis Management Team means specified employees identified in the roles and responsibilities section of the Data Breach Handling Procedure.

Handle in relation to information, means to collect, hold, manage, use or disclose the information.

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

Interference with privacy includes:

(a) acts done, or practice engaged in, by the Shire in contravention of the PRIS Act, in relation to personal information or de-identified information that relates to an individual.

(b) A failure by the Shire to comply in relation to its obligations under the PRIS Act, relating to suspected or assessed notifiable information breaches, that involve personal information.

(c) A failure to comply in relation to a function or activity involving the handling of personal information.

Notifiable Information Breach occurs in the below three circumstances:

(1)(a) There is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity; and

(b) a reasonable person would conclude that the access or disclosure is likely to result in serious harm to any individual to whom the information relates.

(2)(a) If personal information held by an IPP entity is lost in circumstances in which unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and

(b) If the access or disclosure of the information were to occur, a reasonable person would conclude that it would be likely to result in serious harm to any individual to whom the information relates.

(3)(a) If there is unauthorised access to, or unauthorised disclosure of, personal information held by an IPP entity; or

(b) personal information held by an IPP entity is lost; and

(c) the access, disclosure or loss occurs in circumstances set out in a notifiable information breach determination.

Personal information is defined in the PRIS Act as 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 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 is defined in the PRIS Act as personal information that relates to individuals:

- racial or ethnic origin;
- gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth;
- 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;
- health information;
- genetic or genomic information; or
- biometric information.

Relevant policies/documents

Council Policy – Digital Information and Records
Code of Conduct Council Members, Committee Members and Candidates
Employee Code of Conduct
Freedom of Information Statement
Privacy Statement
Organisational Practice - Information Communication and Technology – Information Security
ICT Data Breach Handling Procedure

Relevant legislation/local laws

Freedom of Information Act 1992
Local Government Act 1995
Privacy and Responsible Information Sharing Act 2024
State Records Act 2000

Office use only				
Relevant delegations	Nil			
Council adoption	**Date**	21 April 2026	**Resolution #**	050/2026
Reviewed/modified	**Date**		**Resolution #**	
	Date		**Resolution #**	
	Date		**Resolution #**	
Next review due	**Date**	2030		
