Council Policy – Information Breach

Responsible Directorate	Corporate Services
Responsible Business Unit/s	Information Communication Technology
Responsible Officer	Manger ICT
Affected Business Units	All

Objective

The objective of this Policy is to establish guidelines for the management of information breaches to ensure that the Shire of Serpentine Jarrahdale (Shire) is able to identify, prevent, manage and respond appropriately to information breaches, particularly where they involve personal information.

This Policy supports the Shire's Information Breach Response Plan.

Scope

This Policy applies to:

- all personal information held or handled by the Shire, in any format (electronic, paper, verbal)
- all information assets, systems, applications, and records managed by or on behalf of the Shire
- all employees, contractors, elected members and consultants

This Policy applies regardless of whether the information breach occurs internally, through a third-party service provider, or via an information system managed on the Shire's behalf.

Policy

Explanation

The Shire is committed to protecting personal information and maintaining the trust of the community. Information breaches pose significant legal, operational, reputational, and privacy risks and must be managed promptly and effectively.

The Shire will:

- take reasonable steps to prevent information breaches
- report all suspected or actual information breaches immediately
- assess and respond to information breaches in a timely, consistent and coordinated manner
- comply with all mandatory notification requirements under the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act)
- review and improve controls following an information breach.

Roles and Responsibilities

Employees and Contractors

All employees and contractors must:

- only access personal information required for authorised business purposes
- immediately report any suspected or actual information breach
- comply with this Policy and supporting procedures.

Manager ICT / Incident Response Lead

The Manager ICT (or delegate) is responsible for:

- coordinating the response to information breaches
- ensuring integration with ICT and cyber security incident response processes
- supporting containment, remediation, and investigation activities

Privacy Officer (Chief Executive Officer)

The Privacy Officer (or nominated role) is responsible for:

- assessing whether an information breach is notifiable under the PRIS Act
- coordinating notifications to the Office of the Information Commissioner and affected individuals
- maintaining breach records and reporting obligations.

Executive Management Group (EMG)

EMG is responsible for:

- oversight of significant information breaches
- endorsing notifications where required
- ensuring appropriate resources and controls are in place

Information Breach Preparedness

- Staff will be trained in how to identify, respond to, and manage breaches according to their roles and responsibilities as part of their standard onboarding induction training
- A request can be logged to report an information breach via the Shire website and will be available to Shire staff, elected members, contractors, and the public
- Relevant obligations will be communicated to the Shire's external service providers

Identifying an Information Breach

Information breaches can occur in a wide variety of ways. Each breach will be managed on a case-by-case basis. Breaches may occur due to:

- Accidental disclosure of information
- Deliberate misuse of information
- System misconfiguration

- Cyber attacks

Reporting an Information Breach

All suspected or actual information breaches must be reported immediately through the Shire's ICT Service Desk or directly to Manager ICT or the Coordinator Information Services.

Delays in reporting may increase harm to individuals and expose the Shire to regulatory and reputational risk.

Response to Information Breaches

Information breaches will be managed in accordance with the Shire's Information Breach Response Plan, which outlines procedures for:

- Identification and initial assessment
- Containment and mitigation actions
- Assessment of seriousness and likelihood of harm
- Notification obligations
- Post-incident review and improvement actions

Notification Obligations

Where an information breach occurs where there is unauthorised access to or unauthorised disclosure of personal information and it would be reasonable to conclude that serious harm could result to an individual, the Shire will:

- notify affected individuals as soon as practicable via the Privacy Officer, Manager ICT or Manager Communications depending on the nature of the breach
- provide clear, accurate and timely information about the breach and recommended protective steps

Recordkeeping and Review

The Shire will:

- maintain an Information Breach Register
- maintain comprehensive records of all information breach and near-misses
- use breach information to improve controls, training and systems
- review this Policy annually or earlier if required by legislative or operational change

Non-Compliance

Failure to comply with this Policy may result in disciplinary action and may expose the Shire and individuals to legal consequences under the PRIS Act and other applicable legislation.

Definitions

Information Breach means an information breach occurs when there is unauthorised access to, unauthorised disclosure of, or loss of information, whether intentional or unintentional.

Notifiable Information Breach means an information breach that involves personal information and is assessed as likely to result in serious harm to one or more individuals.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not.

Legislation / Local Law Requirements

- *Privacy and Responsible Information Sharing Act 2024*

Related Documents

- Information Breach Response Plan/Incident Response Plan (E26/4234)
- Council Policy – Privacy (E25/7668)
- ICT Information Security
- Business Operating Procedure (BOP) – Record Keeping
- Information Asset Register
- Business Continuity Plan/Disaster Recovery

Amendment Record

Relevant Delegations		Nil.	
		Date	**Resolution Number**
Council Adoption		**15 June 2026**	**OCM-170-2026**
Version	**Date**	**Resolution Number**	**Amendment Details**