



Governance Policy - 1.15 Information Breach Response Policy

Policy

Governance Policy – 1.15 Information Breach Response Policy

Purpose

The Shire of Peppermint Grove is committed to protecting the confidentiality, integrity and availability of information it holds.

This Policy establishes the framework for identifying, reporting, assessing, managing and responding to information breaches, including notifiable information breaches under the Privacy and Responsible Information Sharing Act 2024 (WA) (PRIS Act). The Policy aims to minimise harm to individuals, ensure compliance with legislative obligations and support continuous improvement in the Shire's information governance practices.

Scope

This Policy applies to all actual, suspected or attempted information breaches involving:

- personal information;
- sensitive personal information;
- confidential information;
- information collected, held or managed by the Shire; and
- information in any format, including electronic, paper, verbal or other media.

This Policy applies to all:

- Elected Members;
- employees;
- contractors;
- consultants;
- volunteers;
- temporary staff;
- agency personnel;
- third-party service providers; and
- any person acting on behalf of the Shire.

Policy Statement

The Shire is committed to ensuring all information breaches are managed promptly, consistently and proportionately.

The Shire will:

- identify and contain information breaches as quickly as practicable;
- minimise harm to affected individuals and the organisation;
- preserve evidence to support investigation and recovery;
- assess each breach to determine its nature, severity and legal obligations;



- notify affected individuals and relevant authorities where required by law;
- maintain accurate records of information breaches;
- implement corrective actions to reduce the likelihood of recurrence; and
- promote continuous improvement through monitoring, review and staff education.

Information Breaches

An information breach occurs where information held by the Shire is accessed, used, disclosed, altered, lost or destroyed without appropriate authority, or where the confidentiality, integrity or availability of information has otherwise been compromised.

Examples of information breaches include:

- an email containing personal information sent to the wrong recipient;
- loss or theft of paper records or portable storage devices;
- unauthorised access to information by staff or third parties;
- cyber security incidents, including malware, ransomware or phishing attacks;
- publication of personal information in error;
- inappropriate disclosure of information during customer interactions;
- contractor or service provider mishandling information; or
- any event that may compromise the security or privacy of information held by the Shire.

Reporting Information Breaches

Any person covered by this Policy who becomes aware of an actual or suspected information breach must report the incident immediately.

Reports must be made to:

- the relevant Manager;
- the Privacy Officer; and
- the Information and Communications Technology (ICT) provider where the incident involves systems, devices, networks or cyber security.

Prompt reporting enables timely containment and assessment and assists the Shire in meeting any legislative notification obligations.

Initial Response

Upon becoming aware of a potential information breach, the Shire will, as soon as reasonably practicable:

- contain the breach and prevent further unauthorised access or disclosure;
- recover information where possible;
- isolate affected systems or devices where necessary;
- disable user accounts or credentials where appropriate;
- preserve logs, records and other evidence relevant to the incident; and
- notify the Privacy Officer to coordinate assessment and response.



Assessment

The Privacy Officer, in consultation with relevant officers, will assess the information breach to determine:

- the nature and cause of the incident;
- the information involved;
- the number of individuals affected;
- whether the information includes sensitive personal information;
- whether the information was encrypted, recovered or publicly available;
- the likelihood and severity of harm to affected individuals;
- whether the incident constitutes a notifiable information breach under the PRIS Act;
- whether legal, cyber security, insurance or other specialist advice is required; and
- any immediate or ongoing risk to the Shire.

Response Team

The response team will be determined according to the nature and severity of the information breach and may include:

- Chief Executive Officer;
- Privacy Officer;
- Manager Corporate Services;
- relevant Service Manager;
- Information and Communications Technology provider;
- Legal Adviser;
- LGIS insurer;
- any other officer or external specialist considered necessary.

Notification

Where required or appropriate under applicable legislation, the Shire will notify:

- the Information Commissioner;
- affected individuals;
- law enforcement agencies;
- insurers;
- cyber security authorities; and
- other relevant regulators or stakeholders.

All notifications will be coordinated by the Privacy Officer and approved by the Chief Executive Officer or delegated officer.

Communications

Only authorised officers may make public or external statements regarding an information breach.

Communications with affected individuals will, where appropriate:

- be timely and accurate;
- explain the nature of the breach;



- outline the likely consequences;
- describe actions taken by the Shire to contain and manage the incident;
- provide advice on actions individuals may take to reduce potential harm; and
- include appropriate contact details for further enquiries.

Information Breach Register

The Shire will maintain an Information Breach Register to record all assessed information breaches and, where appropriate, significant near misses.

The Register will record, at a minimum:

- the date and nature of the breach;
- affected information assets;
- assessment outcomes;
- containment actions;
- notification decisions;
- corrective actions; and
- review outcomes.

Post-Incident Review

Following any significant information breach, the Privacy Officer will coordinate a post-incident review to identify:

- the root cause of the breach;
- lessons learned;
- opportunities to improve policies, procedures and systems.

Related Procedure	Nil
Amended Authority Level	Council
Related Delegation	Nil
Related Local Law/Legislation	Privacy and Responsible Sharing of Information Act 2024 Freedom of Information Act 1992
Adopted	22 September 2026