Data Breach Response

Introduction

The Shire of Toodyay is committed to protecting the personal information of its community, staff, and stakeholders.

This policy outlines Council's strategic commitment to privacy and data protection, and establishes the framework for managing data breaches in accordance with:

- the *Privacy and Responsible Information Sharing Act 2024 (WA)* ("PRIS Act");
- the *Privacy Act 1988 (Cth)*; and
- the *Notifiable Data Breaches Scheme*.

Objective

This policy affirms the Shire's commitment to:

- Upholding the highest standards of privacy and data protection;
- Responding promptly, effectively, and transparently to data breaches;
- Embedding privacy awareness and accountability across the organisation; and
- Ensuring compliance with all relevant privacy legislation and regulatory obligations.

Scope

This Policy applies to all employees; Elected Members; contractors and consultants; volunteers; service providers; and third-party entities who create, access, manage, or handle personal information on behalf of the Shire of Toodyay.

Definitions

Term	Definition
Data Breach	A data breach occurs when personal information held by the Shire is subject to unauthorised access, disclosure, loss, modification, or misuse, resulting in a risk to the confidentiality, integrity, or availability of that information. <u>Examples include:</u> • sending personal data to the wrong recipient; • loss or theft of devices or records; • system compromise, hacking or ransomware • accidental publication or exposure of information; or • unauthorised access to archived or stored records.
Data Breach Classification	Data breaches may include, but are not limited to: • unauthorised access to information; • unauthorised disclosure of information;

Term	Definition
	• loss or theft of records or devices; • unauthorised modification of data; • cyber incidents such as malware or ransomware; or • accidental release or publication of personal information
Notifiable Data Breach	A data breach where unauthorised access, disclosure, or loss of personal information is likely to result in serious harm to an individual, and notification is required under applicable legislation.
Privacy Breach	A privacy breach occurs where personal information is handled in a manner that is inconsistent with applicable privacy legislation or the Information Privacy Principles.
Refer to the Corporate Documents Glossary	https://www.toodyay.wa.gov.au/documents/470/corporate-documents-glossary-(definitions)

1. Policy Statement

Council recognises that the responsible handling of personal information is essential to maintaining public trust and delivering effective services.

The Chief Executive Officer (CEO) is accountable for ensuring that the organisation is prepared for, responds to, and learns from data breaches through the implementation of effective systems, processes, and assurance mechanisms.

This policy is underpinned by the following strategic principles:

- **Trust and Transparency**: The Shire fosters a culture of openness and encourages reporting of data breaches and near misses.
- **Accountability**: Clear roles and responsibilities support timely and effective responses.
- **Integration**: Data breach management is embedded within governance, risk management, and information security frameworks.
- **Continuous Improvement**: Lessons learned are used to strengthen controls, systems, and practices.
- **Community Confidence**: The Shire engages openly with affected individuals to maintain trust.

2. Governance and Oversight

The Chief Executive Officer, in accordance with section 5.41 of the *Local Government Act 1995*, is responsible for ensuring that appropriate systems, procedures, and controls are implemented and maintained to give effect to this policy.

This includes ensuring that:

- a Data Breach Response Plan and supporting procedures are established, maintained, and tested;

- roles and responsibilities for identifying, escalating, and responding to breaches are clearly defined;
- a register of data breaches and near misses is maintained and reviewed;
- breaches are assessed promptly and managed in accordance with legislative obligations;
- notifiable breaches are reported to relevant authorities as required;
- significant data breaches, emerging risks, and trends are reported to Council and the Audit, Risk and Improvement Committee; and
- lessons learned are incorporated into improvements to systems, training, and controls.

3. Data Breach Response Framework

In the event of a data breach, the Shire will implement a structured response to ensure the incident is appropriately managed, risks are mitigated, and statutory obligations are met.

3.1 Identification and Containment

- Identify and confirm the existence of a suspected or actual data breach;
- Immediately contain the breach to prevent further unauthorised access, disclosure, or loss; and
- Secure affected systems, records, or devices.

3.2 Assessment and Risk Evaluation

- Assess the nature and scope of the breach, including:
  - the type of information involved;
  - the sensitivity of the information; and
  - the number of individuals affected.
- Determine the likelihood and severity of harm; and
- Determine whether the breach constitutes a Notifiable Data Breach.

A breach will be considered a Notifiable Data Breach where:

- unauthorised access, disclosure, or loss of personal information has occurred; and
- a reasonable person would conclude that it is likely to result in serious harm to an individual.

3.3 Notification and Reporting

- Report the breach immediately through established internal escalation pathways;
- Notify the CEO as soon as practicable;
- Notify the Office of the Information Commissioner where required by law;
- Notify affected individuals where there is a risk of serious harm; and

- Provide clear and timely information to assist individuals to mitigate impacts.

3.4 Response and Mitigation

- Implement measures to reduce or prevent harm;
- Engage internal and external stakeholders (e.g. ICT providers, legal advisors) as required; and
- Maintain a register of all breaches and actions taken.

3.5 Review and Continuous Improvement

- Conduct a post-incident review to identify root causes;
- Implement corrective actions to strengthen systems, controls, and processes; and
- Update policies, procedures, and training where required.

3.6 Escalation and Reporting to Council

All data breaches must be reported immediately through established escalation pathways.

Significant breaches, including notifiable breaches and systemic risks, will be reported to Council and the Audit, Risk and Improvement Committee in accordance with governance and reporting frameworks.

4. Training and Culture

The Shire will promote a privacy-aware culture through training, awareness campaigns, and leadership engagement.

All employees, contractors, and relevant stakeholders are expected to understand and comply with their responsibilities under this Policy.

5. Review and Revision

This Policy will be reviewed:

- annually or as required;
- following any significant data breach; and
- in response to legislative or regulatory changes.

6. Compliance

Non-compliance with this policy may result in disciplinary action, including termination of employment or contractual arrangements, in accordance with relevant policies and procedures.

7. Contact Information

For inquiries or to report a data breach, contact:

Records Management Officer: records@toodyay.wa.gov.au

8. Effective Date

This Policy is effective from the date of Council approval and remains in force until amended or revoked by Council.

Reference Information

- *Privacy Policy*
- *Privacy Statement*
- *Notifiable Data Breaches Scheme.*
- *Worker's Code of Conduct.*
- *Disclaimer and Copyright Statement*

Legislation

- *Privacy and Responsible Information Sharing legislation*
- *Privacy Act 1988*
- *Freedom of Information Act 1992*
- *Local Government Act 1995*

Associated documents

Notifiable Data Breach Form

Data Breach Register

Document control information	
Document Category	Governance
Document Title	Data Breach Response
Document ID	GOV28 Record D26/12977: Data Breach Response Policy
Document Owner (position title)	Governance Coordinator
Author (position title)	Governance Coordinator
Initial Council Adoption *(including Date and Resolution No.)*	2 July 2026 (CRN: OCM157/07/26)
Last Council Review *(including Date and Resolution No.)*	2 July 2026 (CRN: OCM157/07/26)
Date of Approval	2/07/2026
Approving authority	Council

Document control information	
Absolute or Simple Majority Decision:	Absolute Majority
Access restrictions	Nil
Date Published	28/07/2026
Date of Next Review	Annually or as required