Data Breach Policy

Management

1. Purpose

To provide guidance to Warrumbungle Shire Council (Council) employees in responding to a data breach of Council held information.

This policy and the Data Breach Management Procedure assist with:

- Meeting Council's obligations under the *Privacy Act 1988* (Cth).
- Protection of an important business asset – the personal information of Council's constituents, including but not limited to residents, property owners, staff, councillors, contractors, and visitors to the Warrumbungle local government area.
- Dealing with adverse media or stakeholder attention from a breach or suspected breach.
- Instilling public confidence by responding to a breach systematically and effectively, with the aim of meeting Council obligations and protecting business and personal assets.

2. Scope

This policy applies to all Council employees and contractors. This includes full time, part time, casual, temporary and fixed term employees, agency staff and contractors. For the purposes of this policy, employees also include volunteers, trainees and students on work placements.

3. Associated Policies, Legislation and Documents

ASSOCIATED POLICIES	• Incident and Problem Management Policy • IT and Cyber Security and Usage Policy
ASSOCIATED LEGISLATION	• *Privacy Act 1988* (Cth) • *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) • *Health Records and Information Privacy Act 2022* (NSW) • *Health Records and Information Privacy Code of Practice 2005* (NSW) • *Health Records and Information Privacy Regulation 2012* (NSW) • *Privacy and Personal Information Protection Act 1998* (NSW) • *Privacy and Personal Information Protection Regulation 2014* (NSW)
ASSOCIATED DOCUMENTS	• Agreement for Managed Services – Support and Maintenance, IT End User Support (between Council and Tamworth Regional Council) • Change Management Procedure • Data Breach Management Procedure • Incident and Problem Management Procedure • IT Infrastructure Security Procedure • IT User Access Creation Procedure • Login, Internet and Email Procedure • Privacy Management Plan

4. Definitions

Term	Definition
Confidential information	Information and data (including metadata) including personal information, health information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation. Commercial-in-confidence provisions, floor plans of significant buildings, security classified information, and information related to Council's IT/cyber security systems.
Data breach	For the purpose of this policy, a data breach occurs when there is a failure that has caused unauthorised access to, or disclosure of, confidential information held by Council.
Data breach review team	Comprises the Director Corporate and Community Services, the Manager Corporate Services, and the Coordinator IT Infrastructure and Managed Services (Tamworth Regional Council).
Eligible data breach	A data breach that is likely to result in serious harm to any of the individuals to whom the information related. An eligible data breach arises when the following three criteria are satisfied: 1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; 2. this is likely to result in serious harm to one or more individuals; and 3. the entity has not been able to prevent the likely risk of serious harm with remedial action.
Health information	A specific type of personal information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results.
Likely to occur	The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible).
Personal information	Information or an opinion (including information or an opinion forming part of a database and whether or not in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion This includes, for example, their name, address, email address, phone number, date of birth or photographs.
Reasonable person	A person in Council's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed based on information immediately available or following reasonable enquiries or an assessment of the data breach.

Security classified information	Information and data (including metadata) that is marked as Protected, Secret, or Top Secret as per the Commonwealth Attorney Generals' Department's Protective Security Policy Framework.
Serious harm	In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.
Unauthorised access	Examples include: • an employee browsing customer records without a legitimate purpose • a computer network being compromised by an external attacker resulting in personal information being accessed without authority.

5. Policy

Effective breach management, including notification where warranted, assists Council in avoiding or reducing possible harm to affected individuals/organisations. It also provides the opportunity for lessons to be learned which may prevent future breaches.

In the event of a data breach, Council will form a Data Breach Review Team, whose role it is to investigate, respond and report internally on any known or notified data breach involving confidential information.

Having a data breach response plan is part of establishing robust and effective privacy and information governance procedures (refer to the associated Data Breach Management Procedure). Further, having clear roles and responsibilities is the foundation to a comprehensive and well-managed privacy and information government program.

5.1 Data Breach Definition

A data breach occurs when personal information held by Council is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach may include the loss or theft of a device containing personal information of Council constituents, a Council database or information repository containing personal information being hacked or accessed without authorisation, or Council mistakenly providing personal information to an unauthorised person or entity.

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council data, such as:

- Accidental loss, unauthorised access, or theft of classified material data or equipment on which such data is stored (eg loss of paper record, laptop, iPad or other tablet, or USB stick).
- Unauthorised use, access to, or modification of data or information systems (eg sharing of user login details – deliberately or accidentally – to gain unauthorised access or make unauthorised changes to data or information systems).
- Unauthorised disclosure of classified material information (eg email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent.

- A compromised user account (eg accidental disclosure of user login details through phishing).
- Failed or successful attempts to gain unauthorised access to Council information or information systems.
- Equipment failure.
- Malware infection.
- Disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

5.2 Data Breach Management

Where a data breach is suspected, the General Manager or their delegate must be informed to ensure the application of the Data Breach Management Procedure.

There are four key steps required in responding to a data breach:

1. Contain the breach.
2. Evaluate the associated risks.
3. Consider notifying affected individuals.
4. Prevent a repeat.

Further information on these four steps is set out in the Data Breach Management Procedure.

Council is required to notify the Privacy Commissioner and affected individuals of data breach involving personal or health information that from the perspective of a reasonable person would be likely to result in serious harm (see clause 4 – Definitions).

5.3 Roles and Responsibilities

All employees will:

- Immediately report any actual or suspected data breaches to the Manager Corporate Services.

The Manager Corporate Services will:

- Notify the Director Corporate and Community Services, and IT staff (the Coordinator, IT Infrastructure and Managed Services, and the IT helpdesk) as soon as possible.
- Undertake relevant internal notifications as required by this policy and/or the Data Breach Management Procedure.
- Undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner.
- Notify Council's insurers as required.

IT Staff (Tamworth Regional Council under Agreement for Managed Services)

- Take immediate and any longer-term steps to contain and respond to security threats to Council's IT systems and infrastructure.

6. Getting Help

The staff members who can assist with enquiries about this Policy are:

Position/s: Manager Corporate Services

Department: Corporate and Community Services

7. Version Control

Review Date: By November 2025

Staff Member responsible for Review: Manager Corporate Services

Policy Name	Version	Resolution No.	Date
Data Breach Policy	Endorsed	ELT	1 November 2023