Data Breach Policy GOV-CP-317

(PUBLIC POLICY)

1. Policy History

Revision No.	Council Meeting Date	Minute No.	Adoption Date
1	19/07/2021 (SMT)		
2	23/04/2024	24/114	27/05/2024

2. Policy Objective

This Data Breach Policy has been developed to provide transparency regarding Griffith City Council's process for managing Data Breaches of Council Held Information and to assist Council to meet its legal obligations concerning Mandatory Reporting of Data Breaches under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and Privacy Act.

The objective of this Policy is to outline Council's approach to identifying and managing a Data Breach, including:

- Providing specific examples of incidents considered to constitute a Data Breach.
- Outlining the five essential steps in responding to a Data Breach.
- Addressing the considerations surrounding mandatory or voluntary notification of individuals whose privacy may be affected by a Data Breach. This ensures the Council responds effectively to such incidents.
- Assisting the Council in mitigating potential harm to both the affected individuals and the Council itself.

3. Policy Scope

Council's Data Breach Policy applies to all stakeholders, including Councillors, employees, volunteers, and contractors, and encompasses all activities involving the collection and retention of personal or classified information.

Any individual who suspects that a theft, breach or exposure of Griffith City Council protected data or sensitive data has occurred, must immediately provide a description of what occurred to their Manager and Director.

Any Council staff found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

Council will implement a training initiative designed to educate employees on the potential risks associated with data breaches and to clarify their roles and responsibilities in identifying, addressing, reporting, and preventing such occurrences.

4. Policy Statement

4.1 What is a data breach?

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 or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, tablet or mobile phone, compact disk or USB stick);
- unauthorised use, access to, or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems;
- unauthorised disclosure or misuse of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto Council website without consent;
- compromised user account (e.g. accidental disclosure of user login details through phishing);
- failed or successful attempts to gain unauthorised access to Council IT network 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.

Council is committed to maintaining comprehensive records of all Data Breaches, irrespective of severity or containment status. Effective management of data breaches, including appropriate notification where necessary, is crucial for minimizing potential harm to affected individuals or organizations, safeguarding Council's reputation, and mitigating future breaches.

4.2 What is an ‘eligible’ data breach?

In accordance with the PPIP Act, Council is obligated to notify the Privacy Commissioner and affected individuals of eligible data breaches under the Mandatory Data Breach Notification Scheme.

An eligible data breach is an unauthorised access, disclosure or loss of an individual’s personal information which is likely to result in serious harm to the affected individual.

Determining if a data breach necessitates mandatory reporting obligations involves a dedicated assessment by the Data Breach Response Team, and may also be guided by legal advice.

In assessing seriousness of the breach, the Data Breach Response Team will consider:

- the type of data that has been breached;
- the data context;
- the risk of individuals being identified;
- the circumstances of the breach.

Council's *Data Breach Response Plan* outlines a process to assess eligibility and seriousness so that a risk threshold can be applied to data breach protocols.

4.3 Potential Impacts of a data breach

The impact of a data breach depends on the nature and extent of the breach and the type of information that has been compromised. Some breaches may involve only one or two people while others may affect hundreds or thousands. Larger breaches expose a wider group of people and could require considerable notification and remediation activities. However, it is not only the initial size of the breach that determines its impact. If there is a breach of sensitive or confidential information, reputational and financial harm can occur to both Council and staff.

Serious impacts of a data breach could include:

- risk to individuals' safety;
- financial loss to an individual or organisation;
- damage to personal reputation or position;
- loss of public trust in Council and/or the services it provides;
- commercial risk through disclosure of commercially sensitive information to third parties;
- threat to Council's systems, impacting the capacity to provide services;
- impact on reputation, finances, interests or operation.

Breaches of personal data can result in significant harm, including people having their identities stolen or the private home addresses of protected or vulnerable people being disclosed. In some circumstances, this can expose an individual to a significant risk of harm. As such, even a breach affecting a small number of people may have a large impact.

4.4 Responding to a data breach

The immediate actions taken once a data breach is suspected or identified are crucial in minimising the harm that the data breach could cause. This process will be managed by the Data Breach Response Team, which includes Executive decision makers, information management and technology/security, the Privacy Officer and Communication staff.

The below actions will be undertaken in response to an identified data breach when it occurs:

1. ***Report*** – Any Council Officer who suspects that a data breach has occurred must immediately provide a description to their Manager and Director.
2. ***Contain*** – All necessary steps possible should be taken to contain the breach and minimise any resulting damage.
3. ***Evaluate*** – Assess the type of data involved in the breach, and the risks associated with the breach within 30 days, to determine if there are reasonable grounds to believe that an eligible data breach has occurred. Consider the type of data breach, who is affected, what caused the breach, and what are the specific risks that could follow.
4. ***Notify*** – If on assessment an eligible data breach has occurred, Council will:
    - Notify the NSW Privacy Commissioner and each affected individual
    - Issue a public notification on Council's website where notifying each affected individual is not practicable
    - In instances where Data Breaches involve other public agencies, the General Manager (or delegate) will directly engage with the affected agencies to address any notification requirements for Mandatory Reporting Data Breaches.
    - Notify the OAIC if a Commonwealth Notifiable Data Breach has been identified.
    - Council may consider voluntary data breach notification to the IPC for non-eligible data breaches.
5. ***Act*** – Take all reasonable steps to mitigate the harm done by the suspected breach.
6. ***Prevent*** – Put into action preventative efforts, based on the type and seriousness of the breach. This may include a security audit of both physical and technical security controls, a review of policies and procedures, a review of employee training practices or a review of contractual obligations with contracted service providers. If the breach has been reported to the Privacy Commissioner, further preventative and remedial actions may be recommended subsequent to the Privacy Commissioner's assessment.
7. ***Record*** – Details of the Data Breach incident are to be recorded in Council's Legislative Compliance & Data Breach Register – Record No: 19/35743. Eligible data breaches for which public notifications have been issued will be published in a public notification register on Council's website.

5. Review

Regular reviews, testing, and updates will be conducted for this Policy, following Council's established policy review procedures or prompted by evolving best practices and legislative changes.

6. Definitions

Affected Individual	Means an "affected individual" as defined in the PPIP Act.
Commonwealth Notifiable Data Breach	Means an "eligible data breach" as defined in the Privacy Act.
Council Officer	Means any officer or employee of Council.
Data Breach	A data breach occurs when personal, commercially sensitive or confidential information held by Council is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.
Data Breach Response Plan	A framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by Council in managing a breach if one occurs.
Data Breach Response Team	Nominated Council personnel who are responsible for ensuring that a data breach is managed appropriately.
Eligible data breach	Occurs when there is unauthorised access to, or disclosure of, information, and a reasonable person would conclude that the access or disclosure would likely result in serious harm to any individuals to whom the information relates. Information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, information is likely to occur and, if it did occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any individual to whom the information relates.
Personal Information	Personal information means any information from which a living individual may be uniquely and reliably identified, including an individual's name, Tax File Number (TFN), Medicare number, medical or healthcare data, driver's licence number or associated card information, credit/debit card number, access PIN or Password that would provide access to that individual's financial account or any other non-public personal information
Reasonable person	A phrase frequently used in Tort and Criminal law to denote a hypothetical person in society who exercises average care, skill and judgement in conduct and who serves as a comparative standard for determining liability. Judges since the 19th Century have named the reasonable man as 'the man on the Clapham omnibus". In Australia, NSW courts modified it to "the man on the Bondi tram".
Serious harm	Serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other

	forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

7. Exceptions

Nil

8. Legislation

Griffith City Council is subject to the provisions of the Local Government Act 1993, Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act), Government Information (Public Access) Act 2009 (NSW) GIPA Act and State Records Act 1998 (NSW).

In accordance with the *Privacy and Personal Information Protection Act 1998* (NSW), Council is obligated to notify the Privacy Commissioner and affected individuals of eligible data breaches under the Mandatory Data Breach Notification Scheme (MDBN scheme) from 28 November 2023.

Under the legislation, Council must also publish this policy on its website, along with a data breach incident public notification register.

Under the PPIP Act there are legal obligations which Council must abide by when they collect, store, use or disclose personal information. As exemptions may apply in some instances, it is recommended that staff contact Council's Privacy Officer for further advice.

9. Related Documents

The *Data Breach Response Plan* (GOV-PR-301) is the key document providing Council staff with clear instruction and processes in order to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals.
Other related documents:
(GOV-CP-602) Privacy Policy – Handling of Personal Information
Council's Privacy Management Plan
Legislative Compliance & Data Breach Register
New Public Notification Register

10. Directorate

Economic & Organisational Development