Gwydir Shire Council

Data Breach Policy

Department:	Business Improvement & Information Services
Responsible Manager:	Business Improvement & IT Manager
Date Adopted:	25 October 2023
File Ref:	23/19614
Version No:	1.0
Next Review:	October 2026
Pages:	11

Table Of Contents

1. Overview 3

1.1 Introduction 3

1.2 Purpose 3

1.3 Definitions 3

2. What is an Eligible Data Breach? 4

3. Preparation for Data Breaches 5

3.1 Training and Awareness 5

3.2 Contractors and Third Parties 5

4. Data Breach Response Plan 6

4.1 Report 6

4.2 Contain 7

4.3 Assess 7

4.4 Notify 7

4.4.1 MNDB Notification Requirements 8

4.4.2 NDB Notification Requirements 8

4.5 Review 9

5. Roles and Responsibilities 10

6. Related Documents 11

7. Related Legislation 11

8. Revision Record 11

1. Overview

1.1 Introduction

This Data Breach Policy is established to outline the procedures and responsibilities for managing eligible data breaches in accordance with the federal Privacy Act 1988 (Privacy Act) and the New South Wales Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).

The Privacy Act establishes the Notifiable Data Breaches (NDB) scheme. Under the Under the NDB scheme organisations and must notify affected individuals and the Office of the Australia Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information has been compromised.

In addition to the NDB scheme, the PPIP Act establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches.

1.2 Purpose

The purpose of Gwydir Shire Council's Data Breach Policy is to provide a documented framework that delineates the agency's response procedures in the event of a data breach. This policy sets forth the roles, responsibilities, and specific actions to be taken to effectively address and mitigate breaches of security.

1.3 Definitions

Council Officer	Any officer or employee of Council.
Data Breach	Unauthorised access to, or inadvertent disclosure, access, modification, misuse, or loss of, or interference with Personal Information, and in this Policy includes a potential Data Breach.
IT	Information Technology
Mandatory Reporting Data Breach	Eligible NDB or MNDB data breach.
MNDB Scheme	NSW Mandatory Notification of Data Breach scheme.
NDB Scheme	Notifiable Data Breaches scheme.
OAIC	Office of the Australian Information Commissioner
PPIP Act	*Privacy and Personal Information Protection Act 1988* (NSW).
Privacy Act	*Privacy Act 1998* (Cth).
Privacy Commissioner	NSW Privacy Commissioner, or as otherwise defined in the PPIP Act.
Relevant Manager or Director	The manager or director that a Council Officer reports, or the manager or director with responsibility for a contract with a third-party contractor.
Response Team	The team established for the purposes of responding to a data breach.

2. What is an Eligible Data Breach?

Under the NSW MNDB scheme and the Commonwealth NDB scheme, an organisation or agency must notify affected individuals, the Privacy Commissioner, and the OAIC about an eligible data breach (see section 4.4).

An eligible data breach occurs when there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by Gwydir Shire Council in circumstances likely to result in unauthorised access or disclosure, and a reasonable person would conclude that such access or disclosure would likely result in serious harm to the affected individual(s).

'Harm' caused by a breach can be assessed in number of ways and may be determined based on the following factors:

- Physical safety of the person/organisation
- Financial loss
- Emotional wellbeing/loss
- Reputational damage
- Legal liability
- Breach of secrecy provisions

If Council suspects an eligible data breach may have occurred, it must quickly assess the incident to determine if it is likely to result in serious harm to any individual (see section 4.3).

For further clarification of what constitutes a data breach, see the PPIP Act (section 59D) and the Privacy Act (section 26WE).

Examples of a breach include:

- Accidental loss or theft of Council Held Information or equipment on which such Council Information is stored;
- Unauthorised use, access to or modification of Council Held Information or information systems);
- Unauthorised disclosure of classified Council Held Information, or Council Information posted onto the website without consent;
- A compromised Council Officer's user account;
- Successful attempts to gain unauthorised access to the Council's Information or information systems;
- Malware infection; and
- Malicious disruption to or denial of IT services.

3. Preparation for Data Breaches

Council has a range of supporting policies to control and mitigate exposures to breaches of data. This includes a Cyber Incident Response Plan, Acceptable Use Policy, Password Policy, IT Change Management Policy, and Code of Conduct.

Additionally, Council has established a comprehensive suite of information technology controls. This encompasses access controls, data encryption, security measures for both network and endpoints, systems for preventing data loss, and well-defined plans for responding to incidents. Additionally, the Council diligently maintains an up-to-date record of assets, implementing measures for patching and managing vulnerabilities. This ensures that all IT assets are effectively safeguarded and monitored.

3.1 Training and Awareness

To mitigate the risk of data breaches council has established a training program to educate employees about the risks associated with data breaches and their responsibilities in recognising, responding, reporting, and preventing such incidents. Council conducts regular phishing simulation exercises to assess employee readiness for data breach incidents and raise awareness of the dangers of phishing and social engineering.

3.2 Contractors and Third Parties

Council will require all contracts with contractors who may be provided with, have access to or hold Council Held Information, to contain obligations requiring the contractor to report Data Breaches to Council, take mitigating actions and assist Council in undertaking assessments of the Data Breach. Contracts will also identify who will notify any affected individuals and provide support in the event of a Data Breach.

For Data Breaches that involve other public agencies, the Council will directly liaise with other affected agencies in respect of any notification requirements for Mandatory Reporting Data Breaches.

4. Data Breach Response Plan

There are five steps in the process of responding to a Data Breach, which include:

1. Report
2. Contain
3. Assess
4. Notify
5. Review

As the data breach information is gathered throughout the process, the internal Incident Register should be updated with the following information, as outlined in section 59ZE(2) of the PPIP Act:

- who was notified of the breach,
- when the breach was notified,
- the type of breach,
- details of steps taken by the public sector agency to mitigate harm done by the breach,
- details of the actions taken to prevent future breaches,
- the estimated cost of the breach.

Further, a public notification register will be maintained on Council's website for a minimum of 12 months after the date of publication, as outlined under section 59N(2) of the PPIP Act, and will include the information specified under section 59O.

All actions taken during the process will be thoroughly documented in the document management system of Council, including reports, communications, assessments, and classifications.

Every response will need to be considered holistically, and on a case-by-case basis, depending on the nature, severity, and impact of the Data Breach.

4.1 Report

Any Council Officer who becomes aware of a Data Breach is required to follow the steps outlined below:

- The Council Officer who becomes aware of a Data Breach will immediately notify the relevant Manager or Director.
- It is the responsibility of the Manager or Director to inform the Business Improvement & IT Manager (or delegate), who will assess the breach and determine if it is a mandatory reportable breach (section 4.3).
- If the Business Improvement & IT Manager (or delegate) believes, or has reasonable grounds to believe, that the breach is a mandatory reportable breach, they will promptly notify the General Manager.
- When reporting a possible Mandatory Reporting Data Breach to the General Manager, the notifying party will also indicate whether, in their opinion, it is likely to take more than 30 days to determine if the Data Breach is a Mandatory Reporting Data Breach (if known).

If a data breach is to be determined as non-reportable, the steps will remain the same, except for the “notify” step of the procedure. It will be registered in the internal register, but it will be determined on a case-by-case basis as to who will be notified.

4.2 Contain

As soon as practicable after a potential breach is reported, the Business Improvement & IT Manager should gather the necessary information and complete the Data Breach Incident Report in Council’s incident system and retain any evidence of the breach occurring. A Response Team should be instated to fulfill the roles and responsibilities as outlined in section 5.

Once the type of breach has been identified the Response Team will:

a. For a non-cyber security related breach (e.g., email disclosure to an unintended recipient, hard copy files, verbal disclosure) – take necessary steps to contain and notify;
b. For an IT related breach (e.g., compromised user account, social engineering, ransomware, information and email disclosure to an unintended recipient, hacking) steps will be taken to escalate and implement necessary containment measures in accordance with the Cyber Security Incident Response Plan, minimising harm to individuals and Council.

If a third party is in possession of the personal information and declines to return it, it may be necessary for the Council to seek legal or other advice on what action can be taken to recover the information. When recovering information, the Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

4.3 Assess

The Response Team should review the preliminary assessment carried out by the Business Improvement & IT Manager and complete the Data Breach Response Report in Council’s incident system.

Particular attention should be paid to whether the breach is likely to result in serious harm to any affected parties, as this will determine the implications on Council regarding the notification process.

Council may engage 3rd party assistance or seek advice from the NSW Information and Privacy Commission to provide an opinion or validate the assessment made by the Response Team.

Any further remedial actions identified by the Response Team to contain or minimise the severity of the breach should be taken.

Assessment of the breach should be completed as soon as practicable and at latest within 30 days of the breach being reported.

4.4 Notify

After the Data Breach Incident and Response Report (See Appendix A) has been completed and reviewed by the Response Team and it is determined that Council are required to provide notification of the incident, it is expected that notification will occur as soon as possible. The requirements for the MNDB and NDB are outlined below.

Council will consider other internal and external notifications and approvals and communicate with such external agencies and stakeholders as is reasonably required in the individual circumstances of a particular Data Breach (e.g., the Police, Department of Customer Service, Cyber Security NSW, the Australian Tax Offices etc).

4.4.1 MNDB Notification Requirements

Council's notification requirements for the PPIP Act are listed under section 59N:

59N Public sector agencies must notify certain individuals

(1) As soon as practicable after the head of a public sector agency decides an eligible data breach occurred, the head of the agency must, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify—

(a) each individual to whom the personal information the subject of the breach relates, or

(b) each affected individual.

(2) However, if the head of the agency is unable to notify, or if it is not reasonably practicable for the head of the agency to notify, any or all the individuals specified in subsection (1), the head of the agency must—

(a) publish a notification under section 59P, and

(b) take reasonable steps to publicise the notification.

Section 59M of the PPIP Act requires Council to immediately notify the Privacy Commissioner of an eligible data breach using an approved form. This form can be found on the Information and Privacy Commission NSW website: https://www.ipc.nsw.gov.au/.

The approved form sets out the information that agencies must supply to the Privacy Commissioner when making a notification of an eligible data breach unless it is not reasonably practicable to provide that information.

4.4.2 NDB Notification Requirements

Council's notification requirements for the Privacy Act are listed under section 26WL:

(2) The entity must:

(a) if it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

(b) if it is practicable for the entity to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither paragraph (a) nor (b) applies:

(i) publish a copy of the statement on the entity's website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.

(3) The entity must comply with subsection (2) as soon as practicable after the completion of the preparation of the statement.

Method of providing a statement to an individual

(4) If the entity normally communicates with a particular individual using a particular method, the notification to the individual under paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

Section 26WK of the Privacy Act requires Council to immediately notify the OAIC of an eligible data breach using an approved form. This form can be found on the Office of the Australian Information Commissioner website: https://www.oaic.gov.au/.

The approved form sets out the information that agencies must supply to the Privacy Commissioner when making a notification of an eligible data breach unless it is not reasonably practicable to provide that information.

4.5 Review

After the incident has been assessed and notification has taken place the Business Improvement & IT Manager should carry out a review within 14 days to identify any actions required to prevent further breaches to be tabled at the Senior Management Meeting, covering:

- Recommended changes to system and physical security;
- Recommend changes to any Council policies or procedures;
- Revision or changes recommended to staff training and education.

5. Roles and Responsibilities

Roles and responsibilities are outlined below. The Data Breach response team will generally comprise of staff from these positions.

Position	Responsibilities
Business Improvement & IT Manager	Coordination of preliminary assessment and response team. Provide advice around technical/IT infrastructure security and application data/information security. Implement Incident Response Plan if it is an IT related breach.
Council Staff	Report suspected data breaches to the relevant Director/Manager. Participate in data breach investigations as required. Maintain awareness, prevent breaches, and complete all required cyber security and privacy training as required.
Directors/Managers	To report the data breach as soon as possible to the Business Improvement & IT Manager.
System Owners	Ensure appropriate mechanisms for breach management response is included in all service agreements/contracts related to systems, applications or services that incorporate personal information.
Information Technology Team	Provide advice around technical/IT infrastructure security and application data/information security.
Information Services Officer	Provide advice around records management and compliance.
Legal Counsel	Legal advice.
Risk Officer	Provide risk-based advice and liaise with the insurer as required.
Communications Team	Communications advice.
General Manager	General advice.

6. Related Documents

Acceptable Use Policy

Code of Conduct

Cyber Incident Response Plan

IT Change Management Policy

Password Policy

Privacy Management Plan

7. Related Legislation

Privacy Act 1988

Privacy and Personal Information Protection Act 1998

8. Revision Record

Date	Version	Revision details	Officer	Next Review
Oct 2023	1.0	Initial Document	Justin Hellmuth	Oct 2026