DATA BREACH POLICY

Version No	Created By	Adopted by Council	Review Date
1.0	IT Manager	13 December 2023 Resolution No 2023/247	12 December 2027

Contents

1.0 Introduction

The Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme which requires public sector agencies to notify the Privacy Commissioner and affected individuals of eligible data breaches.

Agencies are required to prepare and publish a Data Breach Policy for managing such breaches as well as maintaining an internal data breach incident register and public register of eligible data breaches.

2.0 Purpose

This policy outlines Council's approach to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and the strategies for containing, assessing and managing eligible data breaches.

3.0 Scope

This policy applies to all Councillors, staff and consultants engaged by Council to perform the role of a public official.

4.0 Related Legislation and Council Documents

Privacy and Personal Information Protection Act 1998
Government Information (Public Access) Act 2009
Health Records and Information Privacy Act 2022
Council's Privacy Management Plan
Council's Business Continuity Plan

5.0 Roles and Responsibilities

The following staff have identified roles under this Policy: -

5.1 General Manager

The General Manager has ultimate responsibility for ensuring Council complies with the MNDB Scheme, authorising any corrective actions and providing a report to the Audit and Risk Management Committee if required.

5.2 Directors

Directors are responsible for receiving notifications of suspected or actual data breaches and coordinating containment of the breach. Directors are also responsible for undertaking an assessment of the suspected or actual data breach and escalating it to the Data Breach Response Team (DBRT) if necessary.

5.3 Data Breach Response Team

The DBRT consists of the Executive Leadership Team and is responsible for determining whether a data breach constitutes an eligible data breach, any notification requirements, fully investigating the cause of the data breach and recommending preventative actions.

5.4 Council Officials

All Council officials have a responsibility for reporting a suspected or actual data breach in accordance with this policy.

6.0 What is a Data Breach?

A data breach occurs when information held by Council (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure. A data breach may occur as a result of malicious action, systems failure, or human error.

Examples of data breaches include: -

6.1 Human Error

- When a letter or email is sent to the wrong recipient
- When system access is incorrectly granted to someone without appropriate authorisation
- When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced
- When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information.

6.2 System Failure

- Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information being sent to incorrect recipients.
- Where systems are not maintained through the application of known and supported patches.

6.3 Malicious or criminal attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
- Social engineering or impersonation leading to inappropriate disclosure of personal information.
- Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
- Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

7.0 What is an Eligible Data Breach?

The MNDB Scheme applies where an eligible data breach has occurred. For a data breach to constitute an eligible data breach: -

- there is unauthorised access to, or unauthorised disclosure of, personal information held by Council or there is a loss of personal information held by Council in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and
- a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

7.1 Personal Information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in material form or not.

Examples of include: -

- Sensitive information – racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record
- health information
- credit information
- employee record information
- tax file number information

7.2 Serious Harm

The term serious harm is not defined in the Privacy and Personal Information Act. Harm that can arise as the result of a data breach is context-specific and will vary based on: -

- the type of personal information accessed, disclosed or lost, and whether a combination of the types of personal information might lead to increased risk
- the level of sensitivity of the personal information accessed, disclosed for lost
- the amount of time the information was exposed or accessible, including the amount of time the information was exposed prior to Council discovering the breach
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)
- the circumstances in which the breach occurred, and
- the actions taken by the agency to reduce the risk of harm following the breach.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that Council would identify as a possible outcome of the breach.

8.0 Systems and processes for managing data breaches

Council has established a range of systems and processes for preventing data breaches. Council's IT network and infrastructure is managed by the Department of Finance and Corporate Strategy who have implemented a number of cyber security measures to mitigate the risk of data breaches. This has included projects to increase cyber security maturity, cyber security training for all staff, data loss prevention, and procedures for the sharing of personal and sensitive information.

Council will ensure all third-party service providers who store personal and health information on behalf of Council are aware of the MNDB Scheme and the obligations under this policy to report any data breaches to Council.

The loss of IT systems as a result of a cyber security incident is included in Council's Business Continuity Plan. Council also conducts cyber security exercises to test the responsiveness of the Business Continuity Plan to a cyber attack and includes cyber security and information security experts in the exercise.

Council established its voluntary Data Breach Response Plan in 2018. The Plan was reviewed in 2022 and is now incorporated into this Policy. This Policy sets out procedures and clear lines of authority for Council staff in the event Council experiences a data breach (or suspects that a data breach has occurred).

9.0 Responding to a Data Breach

There is no single method of responding to a data breach. Data breaches must be dealt with on a case by case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the DBRT may need to include additional staff or external experts, for example an IT specialist/data forensic expert or human resources advisor etc.

When responding to a data breach, the following steps should be considered: -

1. Initial report
2. Contain the breach
3. Assess and mitigate
4. Notify
5. Review

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

9.1 Step One – Initial Report

A suspected data breach may be discovered by a Council staff member, Councillor or third-party provider or Council may be otherwise alerted (e.g., by a member of the public or media).

If an employee becomes aware of, or is notified of a suspected or actual data breach, they must notify their Director within one business day of becoming aware of it and provide information about the type of data breach as detailed in Section 6.0 of the Policy.

Members of the public may also report any data breaches to Council in writing by using the contact details available on Council's website www.narromine.nsw.gov.au.

9.2 Step Two – Contain the breach

The Director should co-ordinate any immediate action to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords. If copies have been made by a third party, ensure that all copies are recovered. This can include receiving written confirmation from a third-party that the copy of the data that they received in error, has been permanently deleted.

9.3 Step Three – Assess and mitigate

The Director will seek the following information about the data breach on order to assess whether the data breach is to be escalated to the DBRT: -

- The date, time, duration and location of the breach
- The type of personal information involved in the breach
- How the breach was discovered and by whom
- The case and extent of the breach
- A list of the affected or possibly affected individuals
- The risk of serious harm to the affected individuals
- The risk of other harm.

Some data breaches may be comparatively minor and be able to be dealt with easily without action from the DBRT e.g., an email sent containing personal information to the wrong recipient. Depending on severity of the contents of the email, if the email can be recalled, or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the response team.

The Director should consider the following questions: -

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in Council's processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the Director decides that a data breach or suspected data breach requires escalation to the DBRT, they must co-ordinate the convening of the response team, ideally on the same working day.

9.4 Step Four – Notify

The DBRT is to determine whether the breach constitutes an eligible data breach. If there are reasonable grounds to believe an eligible data breach has occurred, the DRBT must promptly notify the NSW Privacy Commissioner using the IPC Mandatory Data Breach Reporting Form available online at www.ipc.nsw.gov.au

Individuals/organisations affected by an eligible data breach will be notified as soon as practicable. Where all individuals affected by an eligible data breach cannot be notified, or where direct notification is prohibitively expensive or could cause further harm, the DBRT will consider issuing a public notification.

A record of any public notification of a data breach will be published on Council's website and recorded on the Public Data Breach Register for a period of 12 months.

Notifications should include: -

- The date the breach occurred
- A description of the breach
- How the breach occurred
- The type of breach that occurred
- The personal information included in the breach
- The amount of time the personal information was disclosed for
- Actions that have been taken or are planned to secure the information, or to control and mitigate the harm
- Recommendations about the steps an individual should take in response to the breach
- Information about complaints and reviews of Council's conduct
- The name of the agencies that were subject to the breach
- Contact details for the agency subject to the breach or the nominated person to contact about the breach

The DBRT will also consider whether notification is required to engaging with or notifying external stakeholders (in addition to the NSW Privacy Commissioner), where an eligible data breach occurs. Depending on the circumstances these could include: -

- NSW Police Force, where Council suspects a data breach is a result of criminal activity
- Cyber Security NSW where the data breach is a result of a cyber security incident

- Office of the Australian Information Commissioner where a data breach may involve agencies under Federal jurisdiction
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a data breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers where a data breach may have an impact on these organisations, their functions and their clients.
- Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

9.5 Step Five – Review

The DBRT will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Depending on the nature of the breach this step may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three.

Preventative actions could include a: -

- Review of Council's IT systems and remedial actions to prevent future data breaches
- Security audit of both physical and technical security controls
- Review of policies and procedures
- Review of contractual obligations with contracted service providers

Any recommendations to implement the above preventative actions are to be approved by the General Manager and documented in Council's electronic recordkeeping system.

Consideration will be given to reporting relevant matters to Council's Audit Risk and Improvement Committee.

10. Communication Strategy

Council will aim to notify affected individuals, and external reporting agencies within 5 business days of an eligible data breach of Council information being reported. Notification to individuals will have regard to this Policy (see Appendix B) as well as Council's Privacy Management Plan.

Council's Business Continuity Plan contains template communication messaging for specific incidents including a cyber security incident.

11. Records Management

Documents created by the Director and/or the DBRT, including post breach and testing reviews, should be saved under the following classification in CM9: -

Risk Management – Risk Assessment – Identification and Assessment of Risks

12.0 Testing the Procedures

The DBRT should test the procedures within this policy biennially. This may be done in conjunction with the testing of Council's Business Continuity Plan.

13.0 Policy Review

This Policy will be reviewed regularly to ensure compliance with legislative and regulatory requirements.

Appendix 1 - Data Breach Checklist

STEP 1
Initial Report
(24 hrs)

☐	Employee to notify Director of suspected/actual data breach and type of breach i.e. ☐ Human error ☐ System failure ☐ Malicious or criminal attack

STEP 2
Contain the Breach

☐	Director to immediately coordinate containing breach i.e. ☐ Shutdown system ☐ Recover records ☐ Stop unauthorised practice ☐ Revoke or change access codes or passwords

STEP 3
Assess and Mitigate
(24 hrs)

☐	Director to seek following data breach information ☐ Date, time, duration and location of breach ☐ type of personal information involved in the breach ☐ how the breach was discovered and by whom ☐ the cause and extent of the breach ☐ a list of affected or possibly affected individuals ☐ the risk of serious harm to the affected individuals ☐ the risk of other harm
☐	Director to assess whether data breach is serious enough to escalate to the DBRT. Consider ☐ the number of individuals affected ☐ if there a real risk of serious harm to the affected individuals ☐ if the breach indicates a systemic problem in Council's processes or procedures ☐ the cause and extent of the breach ☐ if there could be media or stakeholder attention as a result
☐	Director to keep appropriate records of suspected breach and actions taken
☐	Director to escalate to DBRT and convene meeting if necessary

STEP 4
Notify
(5 days)

☐	DBRT to determine if breach is an eligible data breach
☐	Notify ☐ Individuals ☐ Public notification ☐ Privacy Commissioner ☐ Other agencies
☐	DBRT to keep appropriate records of eligible data breach and actions taken of DBRT

STEP 5
Review

☐	DBRT to fully investigate cause of the data breach and consider preventative actions ☐ Review of IT systems and remedial actions ☐ Security audit of security controls ☐ Review of policies and procedures ☐ Review of contractual arrangements ☐ Review staff training practices
☐	General Manager to report to Audit Risk and Improvement Committee if necessary

Appendix 2 - Template Notification

Dear (Name)

Council is writing to you with important information about a recent data breach involving your personal information/information about your organisation. Council became aware of this breach on (date).

The breach occurred on or about (date) and occurred as follows: -

- A brief description of what happened.
- Description of the data that was inappropriately accessed, collected, used or disclosed.
- Risk(s) to the individual/organisation caused by the breach.
- Steps the individual/organisation should take to protect themselves from potential harm from the breach.
- A brief description of what Council is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.

We have established a section on our website (insert link) with updated information and links to resources that offer information about this data breach.

We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the (PPIP Act/HRIP Act/GIPA Act) you are entitled to register a complaint with the NSW Privacy Commissioner or NSW Information Commissioner with regard to this breach.

Complaints may be forwarded to the following: -

(insert details)

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me.

Yours faithfully

General Manager