WAVERLEY
COUNCIL

Data Breach Policy

Department	Governance
Approved by	Executive Leadership Team
Date approved	14 November 2024
File reference	A24/0981
Next revision date	Two years from the date of approval or as required due to legislative or regulatory changes or where improvements are identified in response to a data breach whichever occurs sooner
Relevant legislation	*Government Information (Public Access) Act 2009* *Health Records and Information Privacy Act 2002* *Privacy and Personal Information Protection Act 1998* Guide to preparing a data breach policy Guide to managing data breaches in accordance with the PPIP Act
Related policies/ procedures/guidelines	Cyber Security Incident Response Plan - June 2024 (D24/61361) Business Continuity Plans (A22/0044) Privacy Management Plan (D24/110814)
Related forms	N/A

Contents

1. Background

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (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. Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

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

2. Purpose

The purpose of this Data Breach Policy is to provide a clear framework for managing data breaches effectively, ensuring that personal information is protected. The DBP outlines the procedures to be followed in the event of a data breach, including identifying, containing, assessing, and notifying affected parties as well as relevant authorities, such as the NSW Privacy Commissioner. It supports compliance with the Privacy and Personal Information Protection Act 1998 (PPIP Act) and other relevant privacy legislation, with the goal of minimizing the risk and impact of data breaches on individuals and enhancing Council's accountability in handling sensitive information.

3. Scope

This policy applies to all staff and contractors of Council. This includes temporary and casual staff, private contractors and consultants engaged by Council to perform the role of a public official. This policy also applies to third party providers, who hold personal and health information on behalf of Council.

This policy will be reviewed every two years from the date of approval or as required due to legislative or regulatory changes or where improvements are identified in response to a data breach whichever occurs sooner.

4. Content

This DBP specifies Council's approach to managing data breaches, outlining each step of response.

The Policy details:

- What constitutes an eligible data breach under the PPIP Act
- Roles and responsibilities for reporting, reviewing and managing data breaches
- The steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

Effective breach management, including notifications, assists Council in avoiding or reducing possible harm to both the affected individuals/organisations and Council, and may prevent future breaches.

Council acknowledges that not all data breaches will be eligible data breaches but regardless Council takes all data breaches seriously.

4.1 Roles and responsibilities

The following staff have identified roles under the DBP:

- Director Corporate Services is responsible for implementing this Policy, reporting data breaches to General Manager and all notifications and actions for eligible data breaches.
- Executive Manager, Governance is responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches.
- Internal Communications team, People & Culture will provide advice on the internal communication strategy and messaging to and obligations of Council employees; and Corporate Communications Team will provide advice on the external communication strategy and messaging to affected individuals and external reporting agencies.
- All Council employees: all employees have a responsibility for immediately reporting a suspected data breach in accordance with this Policy.

All staff and contractors have a responsibility to notify their supervisor and /or Director Corporate Services of any data breaches within one business day of becoming aware that a data breach has occurred, and the Director of Corporate Services must be informed within five business days of becoming aware that a data breach has occurred and be provided information about the data breach.

4.2 What is an eligible data breach?

The definition of personal information for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act). This means that for the purposes of the MNDB Scheme, *'personal information' means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion and includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.*

A data breach occurs when personal information held by an agency (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.

This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.
A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs).

Examples of data breaches include:

- **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

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

- **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 into 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.

The MNDB Scheme applies where an 'eligible data breach' has occurred. For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are two tests to be satisfied:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and
2. 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.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- The type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- The level of sensitivity of the personal information accessed, disclosed or lost
- The amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency 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
- Actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

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 a reasonable person in the agency's position would identify as a possible outcome of the data breach.

4.3. Systems and processes for managing data breaches

Council has established a range of systems and processes for preventing and managing data breaches.

Council's IT network and infrastructure is managed by Information Management & Technology Department, Corporate Services Directorate, and 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 and awareness, Data loss prevention and procedures for the sharing of personal and sensitive information.

Council will ensure all third-party 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.

This policy establishes a process for reporting, managing and responding to data breaches including notifications to the Privacy Commissioner and affected individuals. The policy also includes steps for reviewing, responding, and developing remedies for preventing data breaches.
Council also maintains an internal register of data breaches and has implemented recommended changes to systems and policies in response to reviewing the causes of data breaches to assist in preventing future breaches.

Presentations and training will be provided Council staff on the MNDB Scheme and reporting and managing privacy and data breaches. Council will continue to review the training needs of staff with respect to privacy and data breaches and provide training in reporting, managing and responding to data breaches.

Council has included the risk of a cyber security incident (which may involve a data breach) within its Risk Register and established controls to mitigate this risk and its impact on the Council's systems, data holdings and individuals. The loss of IT systems as a result of a cyber security incident is included in the Council's Business Continuity Plan.

4.4 Reporting and responding to a data breach

The Director, Corporate Services, must be informed of any data breach to ensure the application of this Policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

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

1. Initial report and triage
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.

Director, Corporate Services or General Manager's nominee will coordinate with Chief Information Officer and/or IT service providers how to address and respond to identified data breaches related to its IT systems.

Step one: Initial report and triage

A staff member, contractor or third-party provider is to notify their Council supervisor and /or Director Corporate Services of any data breaches within one business day of becoming aware that a data breach has occurred.

Director Corporate Services must be informed within five business days of becoming aware that a data breach has occurred and be provided with information about the data breach as detailed in Section 4.2 of this Policy.

Director Corporate Services will notify the General Manager immediately of a suspected eligible data breach.

Director Corporate Services will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme, complete the Data Breach Report and Action Plan and include all data breaches in the Internal Data Breach Register.

Members of the public are also encouraged to report any data breaches to Council in writing by using the contact options available on Council's website.

If a data breach occurs as a result of action from staff within Corporate Services Directorate, Director Corporate Services will immediately notify the General Manager, who will determine whether a Data Breach Response Team will be convened to undertake steps 2-5 in the process of responding to a data breach.

The General Manager may also consider convening a Data Breach Response Team, where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual.

Step two: Contain the breach

Containing the breach is prioritised by Council. All necessary steps possible must be taken 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 a third-party is in possession of the data and declines to return it, it may be necessary for Council to seek legal or other advice on what action can be taken to recover the data. When recovering data, Council will make sure that copies have not been made by a third party or, if they have, 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.

Step three: Assess and mitigate

To determine what other steps are needed, Council will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme, and the risks and potential for serious harm associated with the breach. The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. Director Corporate Services will prepare a report with the proposed actions and recommendations to the General Manager for approval. Data Breach Report and Action Plans are to be saved in Council's electronic record keeping system.

Director Corporate Services will be responsible for the implementation of proposed actions and recommendations.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list.
A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the breach?**

Council's assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- **What was the cause of the breach?**

  Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Questions include: Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?**

  Council's assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information, personal information subject to special restrictions under s.19(1) of the PPIP Act), if could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage Council's reputation?

- **Guidance issued by the Privacy Commissioner on assessing eligible data breaches**

  Upon becoming aware of a possible data breach, Council will take into account any guidance issued by the NSW Privacy Commissioner.

In order to mitigate the breach, Council will consider the following measures:

- Implementation of additional security measures within Council's own systems and processes to limit the potential for misuse of compromised information.
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites.
- Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution to advise caution when relying on identity documents for particular cohorts.

Step four: Notify

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered. There are four elements of the notification process:

1. Undertake a Data Breach self-assessment https://www.ipc.nsw.gov.au/Data-breach-self-assessment-tool. The assessment of the data breach should not be undertaken by a person reasonably suspected of being involved in an action or omission that led to or resulted in the data breach.
2. Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.
3. Determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, Council may not be required to notify affected individuals. The IPC has produced guidance to agencies on exemptions from notification.
4. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
5. Provide further information to the Privacy Commissioner.

Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and is consistent with Council's obligations under MNDB Scheme. Notification demonstrates a commitment to open and transparent governance, consistent with Council's approach. If a data breach is not an eligible data breach under the MNDB Scheme, Council may still consider notifying individuals/organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires Council to take reasonable steps to notify affected individuals as soon as practicable.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

When to notify

Individuals/organisations affected by a data breach will be notified as soon as practicable. Where all individuals affected by an eligible data breach cannot be notified, Council will consider issuing a public notification on its website.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on Council's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). 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 twelve months.

What to say

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

- 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 agency 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.

Other obligations including external engagement or reporting

Council will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs.

Depending on the circumstances of the data breach this could include:

- NSW Police Force and/or Australian Federal Police, where Council suspects a data breach is a result of criminal activity.

- Cyber Security NSW, the Office of Local Government and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident.
- 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.
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

Step five: Review

Council 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 step five may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three above.

Preventative actions could include:

- 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 staff/contractor training practices
- Review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be approved by General Manager and documented in Council's electronic record keeping system. Consideration will be given to reporting relevant matters to Council's Audit, Risk and Improvement Committee.

4.5. Communication strategy

Director, Corporate Services will be responsible for all communications issued under this Policy. Council will aim to notify affected individuals, and external reporting agencies as soon as practicable of a data breach of Council held information being reported to the IPC. Notifications to individuals will have regard for this Policy as well as Council's Privacy Management Plan. Where engagement with external reporting authorities is required, Director Corporate Services will consult Executive Leadership Team members as required.

Council's Cyber Security Incident Response Plan contains template communication messages for specific incidents including a cyber security incident.

5. Review

The DBP will be reviewed every two years from the date of approval or as required due to legislative or regulatory changes or where improvements are identified in response to a data breach whichever occurs sooner.

6. Definitions

Term	Definition
Data breach	A data breach happens when personal information is accessed, disclosed without authorisation or is lost. Under the Notifiable Data Breaches scheme, a person should be informed if a data breach is likely to cause them serious harm.
Health information	'Health information,' defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.
MNDB	refers to the Mandatory Notification of Data Breach (MNDB) Scheme in Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW)
Personal information *Privacy principles*	information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics. Exclusions to the definition of personal information are contained in s4(3) of the PPIP Act and includes health information; (see the definition at s4 PPIP Act and s4(3) PPIP Act and s5 of the HRIP Act). The Information Protection Principles set out in Division 1 of Part 2 of the PPIP Act and Health Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal