Ku-ring-gai Council

Data Breach Policy

Version Number 1

Adopted: 10 February 2024

Effective: 12 February 2024

Data Breach Policy

Table of Contents

Controlled Document Information

Authorisation Details

This is a Controlled Document. Before using this document check it is the latest version by referring to Council's Controlled Document Register. Unless otherwise indicated, printed or downloaded versions of this document are uncontrolled.			
Controlled Document Number:	211	**TRIM Record No:**	2023/348193
Controlled Document Type:	Policy		
Controlled Document Name:	Data Breach Policy		
Version Number:	1		
Department:	Corporate		
Distribution:	Internal and External		
Review Period: **Max < 4 years**	1 year	**Next Review Date:**	28 November 2024
Document Status:	Final		
Approval Type:	Council to adopt / internal for annual review		
Version Start Date:	12.02.2024	**Version End Date:**	27 November 2024

Related Document Information, Standards & References

Related Legislation:	Privacy and Personal Information Protection Act 1998 Health Records and Information Privacy Act 2002	
Related Policies	Business Continuity Management Policy and Framework Computer Access Policy Corporate Credit Card Policy Fraud and Corruption Control Policy Fraud and Corruption Control Strategy Information & Cyber Security Policy Privacy Management Plan Records Management Policy	26 15 115 174 145 186 52
Related Documents	Business Continuity Plans Credit Card Data Handling and Storage Cyber Incident Response Plan	171 182
Other References	NSW Information and Privacy Commission (IPC) Guide - Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy (May 2023) NSW IPC Data Breach Policy (October 2023) NSW IPC Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements (March 2023)	

Version History

Version Number	Version Start Date	Version End Date	Author	Details and Comments
1	12/02/2024	27/11/ 2024	Manager Governance & Strategy	First version created, approved by GMD 23/11/2023, presented to Council 12/12/2023, resolved under resolution 193 to adopt subject to public consultation. No submissions received policy effective 12/02/2024.

Introduction

Purpose and objectives

The NSW Mandatory Notification of Data Breach (MNDB) Scheme requires all NSW public sector agencies to notify the Privacy Commissioner and affected individuals of eligible data breaches. The Scheme aims to:

- protect individuals from the harm caused by identity theft and fraud
- encourage organisations to protect the data that they hold
- help authorities to investigate data breaches.

This policy outlines Ku-ring-gai Council's approach to complying with the MNDB Scheme, reduce the impact of a data breach on affected individuals and Council, and demonstrate to the community that Council takes data security seriously. It provides guidance to staff and the community on how Council will respond to data breaches in accordance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) by setting out the following:

- 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.

Scope

This policy relates to how Council will respond to data breaches. Matters relating to prevention and controls (i.e. risk management, access management, data governance and information security) are covered in related policies and procedures. This policy applies to:

- Council employees
- Councillors
- people employed in the service of Council (e.g. casual staff)
- people providing services or exercising function on behalf of Council, including contractors, subcontractors and volunteers.
- members of Council advisory and reference committees.

This policy also applies to third party providers who hold personal and health information on behalf of Council.

Responsibilities

The **General Manager** is responsible for accepting reports of suspected data breaches, ensuring that an assessment is carried out to determine whether it is an eligible data breach under the MNDB Scheme and ensure that all reasonable efforts are made to contain the breach[1].

The **Director Corporate** is responsible for ensuring that appropriate arrangements and resources are in place to identify, respond, notify and recover from a data breach, approving the data breach report and action plan and keeping Councillors and senior management informed.

The **Manager Information Management** is responsible for containing, investigating and recovering from a cyber incident resulting in a data breach. Further information on roles and responsibilities for responding to a cyber incident are detailed in Council's Cyber Incident Response Plan (internal only).

The **Manager Governance and Corporate Strategy** is responsible for this policy, supporting the investigation of a data breach, ensuring that appropriate record-keeping arrangements are in place, coordinating data breach reports and action plans and maintaining internal and public registers of data breaches.

The **Manager Corporate Communications** will provide advice and support on the communication strategy and messaging to individuals affected by a data breach.

All **Councillors and staff** must report any suspected or actual data breaches to the General Manager, the Information Management team or Governance and Corporate Strategy team.

Response Team

A **Response Team** will be convened to coordinate and manage Council's response to a notifiable data breach. A Response Team may also be convened to manage other breaches that are not likely to result in serious harm. Members of the Response Team will depend on the nature and circumstances of the incident, but may include:

- Manager Information Management
- Key IT systems administrators
- Manager Governance and Corporate Strategy
- Manager Corporate Communications

[1] Note that agency heads have powers to delegate their functions under the MNDB Scheme. These duties are delegated to the Director Corporate, Manager Information Management and Manager Governance and Corporate Strategy.

Council's **Crisis Management Team** (CMT)[2] may also be convened to oversee Council's response to a data breach that is likely to cause serious and widespread harm.

[2] The role of Council's Crisis Management Team (CMT) is to coordinate and respond to events that are likely to have a major or catastrophic impact on Council, organisations or individuals. It is chaired by the Director Operations and includes Council's executive management team (GMD) and key operational managers.

Data breaches

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 data held by Ku-ring-gai Council. The most obvious examples include malware, hacking and data theft, but data breaches may result from a simple human or technical error. Examples of data breaches include:

Human error

- Sending an email to the wrong recipient.
- Granting system access to someone without appropriate authorisation.
- Losing a laptop or other physical asset containing personal information.
- Failing to maintain appropriate password security.

System failure

- System error allowing access to a Council system without authentication.
- Automatically generated notice sent to incorrect recipients.

Malicious or criminal attack

- Cyber incident such as ransomware, malware, hacking, phishing or brute force attack.
- Impersonation leading to inappropriate disclosure of personal information.
- An employee using their credentials to access personal information outside the scope of their duties or permissions.
- Theft of a laptop or other physical asset containing personal information.

Depending on the size and nature of a data breach, the consequences for individuals can be significant. They can lead to financial fraud, identity theft, damage to reputation and even violence.

Data breaches can have serious consequences for Council and other organisations that Council works with. A breach may lead to the disclosure of sensitive information, or otherwise impact on Council's reputation, finances, interests or operations. Ultimately, data breaches can lead to a loss of confidence in Council and the services it provides.

Responding quickly when a breach occurs can substantially reduce its impact on affected individuals, the costs to Council and the potential for reputational damage.

What is an eligible data breach?

The MNDB Scheme requires Ku-ring-gai Council to notify the Privacy Commissioner and affected individuals of **eligible data breaches**. An eligible data breach occurs where:

- there is unauthorised access or disclosure of personal information held by Council, or personal information has been lost in a way that is likely to lead to unauthorised access or disclosure, 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[3].

Breaches can occur between Council and other agencies, within Council or external to Council.

The MNDB scheme applies to breaches of **personal information**, meaning "information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion"[4].

The scheme also applies to **health information** covering personal information about an individual's physical or mental health, disability and information connected to the provision of a health service[5].

The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. However, Council will still take action to respond to the breach and may provide voluntary notification to individuals where appropriate.

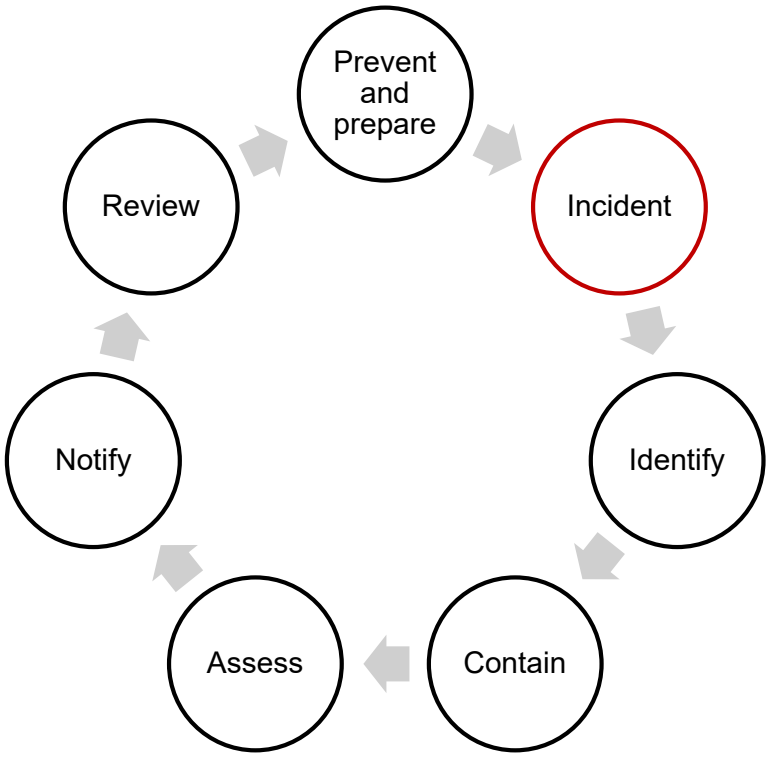
[3] See section 59D of the Privacy and Personal Information Protection Act 1998. Also note that the term "serious harm" is not defined in the Act. Harm that can arise will vary based on the type of information the other circumstances relating to the data breach. Serious harm occurs where there is (or is likely to be) real and substantial detrimental effect to the individual. It must be more than mere irritation, annoyance or inconvenience. Harm to an individual may include (but is not limited to) physical harm, economic / financial harm, emotional / psychological harm or reputational harm.

[4] As defined in section 4 of the Privacy and Personal Information Protection Act 1998.

[5] As defined in section 6 of the Health Records and Information Privacy Act 2002.

Managing a data breach

Ku-ring-gai Council will take the following steps to respond to a reported or suspected data breach.



Council's internal Cyber Incident Response Plan provides staff with step-by-step procedures for a timely and effective response to a cyber incident, from identification through to post-incident review.

Prevent and prepare

Council has a risk management framework in place, and a range of policies and procedures covering the handling of personal and health information, access control, information management and data security. Council has an Information and Cyber Security Policy in place, and a range of supporting policies and procedures to protect its data and mitigate the risk of a data breach.

Under the Data Breach Policy, Council must also ensure that the following prevention and preparation arrangements are in place:

- **Third-party providers:** Council must ensure that third-party providers who store personal and health information on behalf of Council are aware of their obligations under NSW legislation and Council policy. All contracts, memorandums of understanding and non-disclosure agreements include provisions relating to the PIPP Act and the management and notification of data breaches.
- **Training and awareness:** Information on computer access, cyber security, privacy, records management is provided to all staff on induction, and in regular refresher training (at least every two years). This will include information on how to identify a breach, what constitutes an eligible data breach and how to make a report under the MNDB Scheme.
- **Incident response planning:** Council must have a detailed Cyber Incident Response Plan that identifies key roles and responsibilities, communication procedures and steps to be taken to contain, investigate and recover from a cyber incident.
- **Incident response testing:** Council must conduct an annual test of this policy and the Cyber Incident Response Plan.

Identify

A data breach may be identified in a number of ways, including:

- **Unusual system activity:** Information Management and system administrators may detect unusual activity on Council systems, such as a sudden increase in login attempts.
- **System alerts:** Security software may generate alerts indicating that a breach has occurred.
- **Suspicious emails:** Employees may receive suspicious emails, such as phishing emails or emails containing malicious attachments.
- **Customer complaints:** Customers may complain about unusual activity, such as unauthorised charges or suspicious emails claiming to be sent on Council's behalf.
- **Media reports and notifications:** Council may learn about data breaches through media reports or notifications from government authorities, legal representatives or third-party organisations.

How to report a data breach

The MNDB Scheme requires staff with reasonable grounds to suspect that an eligible data breach has occurred to report it.

To minimise the impact of an incident, it is important that that staff report a known or suspected data breach as quickly as possible.

Councillors and Council staff must immediately report a data breach to:

- the General Manager
- Information Management team by phone on 9424 0121, the IM Help Desk (https://helpdesk.kmc.nsw.gov.au) or Kasey Intranet Page (Cyber Security Information), or
- Governance team at governance@krg.nsw.gov.au.

External stakeholders and vendors must immediately report a data breach to:

- the General Manager
- Council's IM Help Desk on 02 9424 0121
- Governance team at governance@krg.nsw.gov.au.

Members of the public should contact Council on 02 9424 0000 or by email at krg@krg.nsw.gov.au.

Assess and contain

Once notified, a **Response Team** will be assembled to contain the data breach, assess the severity of the incident and coordinate a response (in accordance with the Cyber Security Response Plan as appropriate).

Before taking action to contain a data breach, the Response Team will conduct an initial assessment to:

- identify the scope of the data breach, including the type of data affected, the affected systems or applications and the potential number of individuals impacted.
- rate the severity of the data breach, considering the sensitivity of the data, the likelihood of unauthorised access or disclosure, and the potential impact on affected individuals.

The immediate priority of the Response Team will then be to contain the data breach. Depending on the type of incident, containment may involve:

- isolating affected systems and networks from the internet and internal networks to prevent further unauthorised access or data loss following a malicious attack
- restricting access to affected systems and data, by changing passwords or revoking access
- wiping or resetting lost devices to prevent unauthorised tampering or data extraction
- notifying staff, stakeholders and third-party vendors of the incident and any precautions they need to take.

The Response Team must carry out an assessment of whether there are reasonable grounds to believe that it is an **eligible data breach**. This assessment must be completed within 30 days[6]. Once it is determined that an eligible data breach has occurred, the notification process under the MNDB Scheme is triggered (see the following section of this policy).

The Response Team will collect evidence, system logs and other data related to the breach, and investigate vulnerabilities or errors that led to the compromise. This will be crucial for understanding the root cause, confirming the scope and severity of the incident and determining whether it is an eligible data breach.

The Response Team must document and register all actions taken during the assessment and containment phase, including personnel involved and the specific steps taken.

[6] In accordance with section 59E(2)(b) of the Privacy and Personal Information Protection Act 1998

Further details on the steps Council will undertake to assess and contain a cyber incident are included in Council's Cyber Incident Response Plan.

Notify

If an **eligible data breach** has occurred, the notification process under the MNDB Scheme (Part 6A of the PPIP Act) is triggered. Council must notify both the Privacy Commissioner and affected individuals of an eligible data breach.

Step 1: Notify the Privacy Commissioner

Council must notify the Privacy Commissioner immediately[7] after an eligible data breach is identified using the approved form (available from the NSW IPC here).

Step 2: Determine if an exemption applies

Council will determine whether an exemption applies. If one of the exemptions set out in the MNDB Scheme applies, Council may not be required to notify affected individuals. These exemptions are where:

- a breach involved multiple agencies and another agency has undertaken to provide the notification.
- notification would likely prejudice an investigation or court or tribunal proceedings.
- mitigation action taken by Council has prevented any likely serious harm resulting from the breach.
- notification would be inconsistent with a secrecy provision in another Act.
- notification would create a serious risk of harm to an individual's health or safety.
- notification would compromise the Council's cyber security or lead to further breaches.

See **Appendix A** for further information on exemptions under the PIPP Act.

Step 3: Notify affected individuals and organisations

Unless an exemption applies, Council will notify affected individuals or their authorised representative as soon as reasonably practicable to enable them to take steps to protect themselves. Notification should be within 5 business days of determining that it is an eligible data breach.

Affected individuals and organisations will be notified directly (i.e. by telephone, letter or email) where practicable.

[7] In accordance with section 59M of the Privacy and Personal Information Protection Act 1998

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 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.

Council will provide a public notification (i.e. by media release) where the contact details are not known or where direct notification is prohibitively expensive. All public notifications must be included on Council's public notification register on the website.

Step 4: Notify law enforcement and/or other external stakeholders

Council will also consider whether notification or other actions are required under state and Federal law, contractual or other administrative arrangements. Depending on the circumstances of the data breach this could include the following:

- Notifying the NSW Police where a data breach may be a result of criminal activity.
- Notifying Cyber Security NSW where a data breach is a result of a cyber security incident.
- The 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.
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

Step 5: Update the Privacy Commissioner

Council will provide a follow-up notification to the Privacy Commissioner of any information that was not included in the original notification, as the breach response progresses, and as new information comes to light[8]. This will include a link to any notification on Council's public register.

Voluntary notification

The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. However, Council will still take action to respond to the breach and may provide voluntary notification to individuals where appropriate.

[8] In accordance with section 59Q of the Privacy and Personal Information Protection Act 1998

Review

Council will complete an investigation of the circumstances of an eligible data breach to determine root causes and what actions should be taken to prevent any reoccurrence. Preventative actions could include a review of:

- IT systems and security controls
- policies, procedures or training provided to staff
- contractual obligations with contracted service providers.

Reporting and recordkeeping

A full report of the data breach and action plan to implement preventative actions must be approved by the Director Corporate and reported to Council's Audit, Risk and Improvement Committee (ARIC).

The Response Team must document and register all actions taken during the assessment and containment phase, including personnel involved and the specific steps taken.

The data breach report, action plan and all records relating to the management of the breach are to be registered and saved in Content Manager.

Data breach incident register

Each eligible data breach must be entered on Council's internal incident register 2024/067462.

Maintaining the incident register is important for record-keeping and reporting purposes, as well as to comply with any request for information from the Privacy Commissioner.

Testing and updating

The process outlined in this policy will only be effective if it is kept up to date. To ensure that Council's response plan reflects changes in the internal and external environment, Council will conduct a test exercise, review and update this policy and the Cyber Incident Response Plan as part of its regular business continuity testing.

Appendix A: Exemptions from notification requirements

Part 6A, Division 4 of the PPIP Act provides a limited number of exemptions from the requirement to notify affected individuals of an eligible data breach. Council is not required to notify where any of the following exemptions apply[9].

Breaches involving multiple agencies

The exemption under section 59S will apply where:

- the data breach involves more than one agency
- each agency has undertaken an assessment of the breach,
- the head of each agency has made a data breach notification to the Privacy Commissioner, and
- the other agency involved in the breach has undertaken to notify affected individuals of the eligible data breach.

In this case, Council will work with other agencies during the assessment process to ensure all affected individuals are identified. The notification provided to the affected individuals should identify all agencies involved in the breach. The notification should also identify a central contact for further enquiries.

This exemption does not apply where multiple entities were involved in the breach, but Council is the only NSW public sector agency (as defined under the PIPP Act). In this instance, Council will need to comply with the notification requirements even if another entity (including an agency of the Commonwealth or another state or territory) was also required to notify affected individuals under Commonwealth or other law.

Investigations and legal proceedings

The exemption under section 59T will apply where Council reasonably believes notification would likely prejudice:

- an investigation that could lead to the prosecution of an offence
- proceedings before a court or tribunal
- another matter prescribed by regulations.

[9] Source: NSW Information and Privacy Commission Fact Sheet: Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements (March 2023)

Mitigation of harm

The exemption under section 59U will apply where Council:

- takes action to mitigate the harm done by the breach, and
- the action is taken before the breach results in serious harm to an individual, and
- because of the action taken, a reasonable person would conclude that the breach would not be likely to result in serious harm to the individual.

The time period for when this exemption could apply is after Council has determined that the breach is an eligible data breach but before the breach results in serious harm to the individual.

Secrecy provisions

The exemption under section 59V will apply where compliance with the notification requirements would be inconsistent with a secrecy provision. For the purposes of the MNDB Scheme, a secrecy provision means a provision of an Act or statutory rule that prohibits or regulates the use or disclosure of information.

Serious risk of harm to health or safety

The exemption under section 59W will apply where the Council reasonably believes that notification would create a serious risk of harm to an individual's health or safety. When considering whether to apply this exemption, Council must have regard to the Privacy Commissioner's Guideline on the exemption under section 59W. When making a decision to apply this exemption Council must:

- consider the extent to which the harm that may be caused by notifying the individual is greater than the harm of not notifying the individual about the breach, and
- consider the currency of the information relied on in assessing the serious risk of harm to the individual, and
- must not search data held by the agency that was not affected by the data breach during the assessment of risk unless the agency knows, or reasonably believes, there is information in the data that is relevant to whether the exemption applies.

This exemption can be applied permanently, temporarily or until a particular event has occurred. The type of exemption applied will depend on the nature and context of the breach and the unique characteristics and circumstances of the affected individual.

Council must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59W(5).

Cyber security

The exemption under section 59X will apply where Council reasonably believes that notification would worsen the Council's cyber security or lead to further data breaches.

When considering whether to apply this exemption Council must have regard to the Privacy Commissioner's Guideline on the exemption under section 59X.

This exemption can only be applied on a temporary basis for the duration of the risk to the Council's cyber security.

Council must provide a written notice to the Privacy Commissioner where this exemption is relied upon. The notice must include the information specified under section 59X(3).

Council must review the use of this exemption each month and provide an update to the Privacy Commissioner

Notification to the Privacy Commissioner

These exemptions do not affect Council's obligation to make a notification to the Privacy Commissioner under section 59M.