CUMBERLAND
CITY COUNCIL

Data Breach Response Policy

DRAFT

AUTHORISATION & VERSION CONTROL

Policy Number	POL-053
Policy Owner	Director Governance & Risk
Date Adopted	(Approval Date)
Version No	2.0
Document ID Number:	(ECM Reference Number)
Review Date	(Review Date)

BACKGROUND

As of 22 February 2018, the Notifiable Data Breaches (NDB) scheme came into effect under the federal *Privacy Act 1988* (Privacy Act). 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, amendments to the *Privacy and Personal Information Protection Act 1998* (PPIP Act) are effective as of 28 November 2023 creating a Mandatory Notification of Data Breach (MNDB) Scheme which requires public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Cumberland City Council maintains personal information such as ratepayer, resident and customer data/information from parties who interact with Council. Council also maintains personal and workforce data/information. This data is collected by Council as is used to plan, monitor and manage the workforce, services and properties across the Local Government Area (LGA).

Council must comply with the notification requirements of the scheme in the event of any data breach occurring as failure to do so may render Council liable for significant penalties under Australian law.

DEFINITIONS

Act	*Local Government Act 1993.*
Commercial Information	Any commercial information, whether it be that of Council's, external stakeholders or provided by a service provider/service partner in confidence. Note that commercial information does not fall within the MNDB scheme unless it contains Personal Information or Health Information.
Confidential Information	Information and data including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of residential buildings, Security Classified Information and information related to Council's IT/cyber security systems.
Councillor	Cumberland City Council elected representative.
Council committee member	A person other than a Councillor or a Council Officer who is a member of a Council committee other than a wholly advisory committee, and a person other than a Councillor who is a member of Council's audit, risk and improvement committee.
Council Official	Councillors, Council Officers, Council committee members and delegates of Council.
Council Officer	Cumberland City Council members of staff (including full-time, part-time, casual and contracted staff).
Data Breach	A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

DRAFT

Eligible Data Breach	A Data Breach that would be likely to result in serious harm to an individual to whom the information that is the subject of the Data Breach relates.
Health Information	Information or an opinion about a person's physical or mental health or disability, or information relating to the provision of health services to a person. Health information can include a psychological report, blood tests or an x-ray, results from drug and alcohol tests, information about a person's medical appointments, and information regarding vaccination status. It can also include some personal information that is collected to provide a health service, such as a name and telephone number. For the purposes of the MNDB scheme, Health Information is Personal Information.
MNDB scheme	Mandatory Notification of Data Breach scheme in New South Wales.
NDB scheme	Notification of Data Breach scheme in Australia.
Personal Information	Information or an opinion about a person where that person's identity is apparent or can reasonably be ascertained. This information can be in a database and does not necessarily have to be recorded in a material form. For the purposes of the MNDB scheme, Personal Information includes Health Information.

PURPOSE

The purpose of this policy is to provide a procedure detailing the key actions and responsibilities to be followed in the event of a data breach incident.

SCOPE

The scope of this policy applies to all data held by Council in either a paper based or electronic format and is applicable to all employees (including councillors, contractors, students, volunteers and agency personnel) as well as external organisations and contractors who have been granted access to Council's infrastructure, services and data.

This Policy supplements Cumberland City Council's Privacy Management Plan.

WHAT IS A DATA BREACH?

A Data Breach is an incident where an unauthorised access to, or unauthorised disclosure or loss of, Personal Information, Health Information or Commercial Information has occurred. The information may have been compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen, or used by unauthorised individuals, whether accidentally or intentionally.

Examples of a Data Breach include:

- A database that contains individuals' Personal Information has been accessed by an unauthorised person.
- Personal information held by Council is disclosed by an unauthorised person.
- A device containing Personal Information or Commercial Information is lost or stolen.
- A cyber attack has occurred which has resulted in stolen Personal Information.

DRAFT

Processes for identifying and reporting breaches

Council may be made aware of a data breach through a report from a member of staff, a contractor, an affected third party or through a report from another government agency. Council may also receive a written request seeking an internal review of a privacy complaint relating to a data breach incident. In the event of a known or suspected data breach, this should be reported either verbally or in writing to Council's Manager Governance as soon as practicable who will commence the response process.

Data Breaches may also be identified by a cyber security incident such as malware, a hacking attack, ransomware, denial of services, phishing attack or a combination of these. Council several systems in place for the identification of Data Breaches, including comprehensive cyber security, security systems and auditing requirements.

When does a breach become 'eligible' for notification

Under the Mandatory Notifiable Data Breach (MNDB) scheme an organisation or agency must notify affected individuals and the NSW Privacy Commissioner about an eligible data breach. An 'eligible data breach' occurs where:

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.

'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

Data Breach Preparation and Prevention Measures

To minimise the risks associated with Data Breaches, Council undertakes and implements the following measures:

- Ensures that Council Officers receive a copy of the Data Breach Response Policy when they commence employment at Council.
- Provides training and targeted advice to Council Officers and business units to help them understand how the Data Breach Response Policy is implemented.
- Encourages Council Officers to seek advice from the relevant officers in Council in relation to any potential data breach issues or concerns.
- Promotes awareness and compliance with Data Breach requirements by participating in promotional activities as part of the annual Privacy Awareness Week.

DRAFT

- Ensures that service providers/service partners are aware of their obligations under this Policy to report any Data Breaches to the Manager Governance or Director Governance & Risk immediately.
- Schedules for regular testing to assess the effectiveness of Council's response to Data Breaches, and to assess whether there are any risks which need to be addressed.

Data Breach Response Strategy

Following the report of a Data Breach, the Response Team must conduct a four-step response process as expeditiously as possible. These four steps include containing, assessing, managing, reporting, and reviewing the Data Breach.

1. **Containment**

- As soon as practicable after a potential breach is reported, the Manager Governance should gather the necessary information and complete the Data Breach Incident and Response Report - Part A (See Appendix A) and retain any evidence of the breach occurring.
- Necessary steps should be taken by the Manager Governance immediately to contain the breach once details of the incident have been gathered (this may involve coordinating with other members of staff to ensure necessary steps/measures are put in place). Steps may involve recovering information, suspending, or shutting down the breach system, revoking or changing access.
- Once a preliminary assessment of the level of risk posed by the breach (high, medium, low) has been established, the Response Team is to be notified and a time arranged to assess the breach.

2. **Assessment and Evaluation**

- The Response Team should review the preliminary assessment carried out by the Manager Governance and complete the Data Breach Incident and Response Report - Part B (See Appendix A).
- The Response Team will assess the type of information affected by the breach, who is affected, the cause, any foreseeable harm to any affected parties and any other necessary factors.
- Council may engage third 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.
- The Response Team must notify other organisations if required, such as the NSW Police Force in the case of theft, or the Australian Cybercrime Online Reporting Network in the event of a cyber attack.
- Assessment of the breach should be completed as soon as practicable and at latest within 30 days of the breach being reported.

3. **Notification and Reporting**

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 is legally obliged to provide notification of the incident – it is expected that notification occurs within 72 hours of the assessment being made.

DRAFT

Reporting to the NSW Privacy Commissioner

Where it has been determined that an Eligible Data Breach has occurred, or that there is reasonable ground to believe that an Eligible Data Breach has occurred, Council will immediately notify the NSW Privacy Commissioner via the Data Breach Notification to the Privacy Commissioner Form.

Reporting to the Australian Privacy Commissioner (Commonwealth Notifiable Data Breach)

The *Privacy Act 1998* (Cth) requires Council to report to the Australian Privacy Commissioner instances where a Data Breach affects the tax file number of individual/s. If this occurs, the Council will immediately notify the Australian Privacy Commissioner via the Notifiable Data Breach Form.

Reporting to the affected individual or organisation

Council will notify each individual or organisation to whom an Eligible Data Breach relates, and provide them with information about the Eligible Data Breach. Where a Data Breach is not an Eligible Data Breach, Council may still provide voluntary notification to individuals and organisations where appropriate. Council will publish a public notification of the Data Breach if it is not reasonably practicable to inform each individual or organisation, or if the Council otherwise deems it appropriate. After the public notification of an Eligible Data Breach is published, Council will inform the NSW Privacy Commissioner of how to access the notification.

4. Reviewing and Monitoring

After the incident has been assessed and notification has taken place, the Director Governance & Risk will coordinate a further investigation into the circumstances of the breach to ensure that any processes or weaknesses in data handling that may have contributed to the Data Breach are identified and remediated. This will mitigate future risks and ensure Council's proactive management of Data Breaches.

The investigation findings and recommendations must be reported to the Executive Team and cover the following:

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

Recordkeeping Requirements

Data Breach Register

Council will maintain an internal Data Breach Register which details the following:

- Who was notified of the Data Breach
- When the Data Breach was notified
- The type of Data Breach
- The steps taken by Council to mitigate the harm done by the Data Breach
- Details of the actions taken to prevent future Data Breaches
- The estimated cost of the Data Breach.

DRAFT

Public Notification Register

Council will keep a public notification register that is available on its website. The public notification register will contain details of the Data Breaches that have been notified to the public, including all information provided to an individual or organisation when they are notified of a Data Breach. Personal Information or information that could prejudice Council's functions will not be published on the public notification register. Data Breaches published on the public notification register will remain on the register for at least 12 months.

ROLES & RESPONSIBILITIES

- Council Officials, volunteers, service providers/service partners and members of the public are responsible for immediately reporting any actual or suspected data breaches to the Manager Governance or Director Governance & Risk.

- The Data Breach Response Team is responsible for the following:
    - Immediately meeting to review and respond to the reported Data Breach, with delineation of responsibilities undertaken depending on the nature of the Data Breach.
    - Following the response requirements as set out in this Data Breach Response Policy.
    - Consulting with relevant internal and external stakeholders as required.
    - Assisting the Director Governance and Risk with the notification requirements.

The Data Breach Response Team will generally comprise of staff in the following positions:

Position	**Responsibilities**
Director Governance & Risk	Oversight of Council's obligations being met under this Policy. Provision of advice as required. Also responsible for liaison and reporting with relevant oversight agencies.
Manager Governance	General governance, compliance and records management advice and coordination of preliminary assessment and response teams including completion of reports at Appendix A
Executive Manager Customer Experience and Technology	Provide advice around application level data/information security
Senior Coordinator Technology Services	Provide advice around technical/IT infrastructure security
Internal Ombudsman	Process oversight, quality assurance
General Counsel	Legal advice
Manager Strategic Communications	Communications advice
Director Corporate Performance	General advice and direct linkage to executive
General Manager (High Risk Only)	General advice

DRAFT

RELATED DOCUMENTS AND COUNCIL POLICY

- Code of Conduct
- Privacy Management Plan
- Risk Management Policy

RELATED LEGISLATION

- *Privacy Act 1988 (Privacy Act)*
- *Local Government Act 1993*
- *Government Information (Public Access) Act 2009*
- *Government Information (Public Access) Regulation 2018*
- *State Records Act 1998*
- *Privacy and Personal Information Protection Act 1998*
- *Privacy and Personal Information Protection Amendment Act 2022*
- *Health Records and Information Privacy Act 2002*

DRAFT

APPENDIX

Appendix A – Data Breach Incident & Response Report

Part A – Data Breach Incident Report

To be completed by the Manager Governance on receipt of breach report

<table>
<tr><td>Name/Position:</td><td>Date:</td></tr>
<tr><td colspan="2">When, where and how did the breach occur?</td></tr>
<tr><td colspan="2">Who and how was the breach discovered?</td></tr>
<tr><td colspan="2">When the breach was first reported?</td></tr>
<tr><td>How would you classify the breach?

o Unauthorised access
o Unauthorised disclosure
o Loss
o Alteration
o Destruction of personal information</td><td>What information/data has been compromised?

o Financial details
o Tax File Number
o Identity Information
o Contact Information
o Health Information
o Other</td></tr>
<tr><td colspan="2">What parties have been affected by the breach?</td></tr>
<tr><td colspan="2">Steps taken to immediately contain the breach?</td></tr>
<tr><td colspan="2">Have any external parties been notified about the breach? E.g. The OAIC, NSW Information and Privacy Commission, Police, Insurance providers, credit card companies etc</td></tr>
<tr><td colspan="2">Preliminary Assessment of risk posed by the data breach?

o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation
o Moderate Risk
o Low Risk</td></tr>
</table>

DRAFT

Part B – Data Breach Response Report

To be completed by the Manager Governance at completion of the Response Team's assessment meeting.

Name/Position:	**Date:**
List the response team members	
Listing of preliminary steps that have been taken to contain the breach	
Any further steps identified to minimise the impact on affected individuals or organisations?	
Validation of risk posed by the data breach? o High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation o Moderate Risk o Low Risk	
Confirmation of notification required o MNDB Eligible data breach – mandatory disclosure (high risk) o Council elected voluntary disclosure (low or medium risk) o GDPR data breach – mandatory disclosure required within 72 hours (high, medium or low risk)	
Agencies notified o OAIC o NSW Information and Privacy Commission	
Confirmation of Notification Approach o Directly notify only those individuals at risk of serious harm, or o Directly notify all individuals whose data was breached, o Publicise the statement more broadly. Please specify whether notification is to occur via phone, letter, email or in person.	
Next steps for Review phase	

DRAFT