Data Breach Policy

December 2023

newcastle.nsw.gov.au

City of Newcastle

Table of Contents

Part A Preliminary

1 Introduction

1.1 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 NSW public sector agencies bound by the PPIP Act, including City of Newcastle (CN), to notify the Privacy Commissioner and affected individuals of Eligible Data Breaches.

1.2 Under the MNDB Scheme, CN is required to:

a) Prepare and publish a Data Breach Policy (the Policy); and

b) Maintain an internal register and public register of Eligible Data Breaches.

2 Purpose

2.1 The purpose of this Policy is to set out how CN will manage and report Eligible Data Breaches.

3 Scope

3.1 This Policy applies to all CN Staff, Councillors, volunteers, contractors and third party providers, who hold Personal Information on behalf of CN.

3.2 A breach of this Policy is a breach of CN's Code of Conduct.

4 Principles

4.1 CN commits itself to the following:

a) **Accountability and transparency** - This Policy provides a framework for the transparent handling and management of Eligible Data Breach and accountability to individuals affected by an Eligible Data Breach.

b) **Alignment with Council strategies** - This Policy aligns with Council priorities outlined in the Newcastle Strategic Plan.

Part B Managing and reporting data breaches

5 What is a data breach for the purposes of this Policy?

5.1 A data breach occurs when Personal Information held by CN (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.

5.2 Examples of data breaches include:

a) Human error or deliberate misuse

i. When a letter or email is sent to the wrong recipient.
ii. When system access is incorrectly granted to someone without appropriate authorisation.
iii. When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
iv. When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
v. When staff accesses or shares Personal Information where the staff or team do not require the Personal Information to do their job

b) System failure

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

c) Malicious or criminal attack

i. Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
ii. Social engineering or impersonation leading into inappropriate disclosure of personal information.
iii. Insider threats from staff 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.

5.3 This Policy applies to an Eligible Data Breaches only. For a data breach to meet the criteria of an Eligible Data Breach there are **two tests that must both be satisfied:**

a) Test One

i. there is unauthorised access to, or unauthorised disclosure of, Personal Information held by CN; or
ii. there is a loss of personal information held by CN in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

b) Test Two

i. 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.

Note: the term 'serious harm' is not defined in the PPIP Act. 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.

c) In determining serious harm in accordance with Test Two, CN will have regard to:

i. the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk;

ii. the level of sensitivity of the personal information accessed, disclosed or lost;

iii. 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;

iv. 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);

v. the circumstances in which the breach occurred; and

vi. actions taken by CN to reduce the risk of harm following the breach.

6 Systems and processes for preventing data breaches

6.1 The scope of this Policy does include controls for systems and processes preventing data breaches.

6.2 CN has established a range of systems and system processes for preventing data breaches.

a) In addition, CN has included the risk of a cyber security incident (which may involve a data breach) as a risk in its Risk Register and established controls to mitigate this risk. CN has in place a Business Continuity Plan to respond in the instance of a cyber attack impacting CN's systems.

7 Register of data breaches

7.1 CN maintains an internal register and public register of Eligible Data Breaches.

8 Training and awareness

8.1 All CN Staff will receive training in privacy management including the reporting and notification of data breaches.

9 Reporting and responding to an Eligible Data Breach

9.1 In the instance of an Eligible Data Breach, CN will take steps to report, contain, assess and mitigate the impact of the breach.

9.2 CN will manage Eligible Data Breaches in accordance with CN's Cyber Incident Response Plan (CIRP) in accordance with established policy and procedures. There are five key steps CN will take in responding to a data breach:

a) <u>Step one: Initial report and triage</u>

When CN receives a report of a possible Eligible Data Breach, the Executive

Director Corporate Services will review and triage the report and determine under the Crisis and Emergency Management Plan (CEMP) whether to stand up an Incident Management Team and enact the relevant Business Continuity Plan (BCP).

b) Step two: Contain the breach

CN will prioritise containing the breach.

For example, recover Personal Information, shut down a system that has been breached or suspend an activity or take steps or seek advice on steps to be taken where a third-party is in possession of Personal Information.

c) Step three: Assess and mitigate

To determine the approach to managing a breach, CN will:

i. undertake an assessment of the type of data involved in the breach; and
ii. complete a risk assessment including an assessment of serious harm associated with the breach.

Where the breach is determined to be an Eligible Breach causing serious harm, CN will:

i. Undertake an investigation; and
ii. Complete a Data Breach Report and Action Plan including seek advice from the Information & Privacy Coordinator and reporting to the Executive Director Corporate Services who will be responsible for the implementation of proposed actions and recommendations.

Factors to considered in Data Breach Report and Action Plan. The CN assessment will include reviewing considering:

i. Who is affected by the breach?
   - Who - is it individuals and organisations;
   - How many;
   - The risk - whether any of the individuals have personal circumstances; or which may put them at particular risk of harm.
ii. What was the cause of the breach?
   - Whether the breach occurred as part of a targeted attack or through inadvertent oversight; and
   - The foreseeable harm to the affected individuals/organisations?

d) Step four: Notify and communicate

If after following steps 1-3, it is determined that an Eligible Data Breach has occurred, the notification process under Division 3 of the Mandatory Notification of Data Breach Scheme (Part 6A of the PPIP Act) is triggered. CN's Privacy & Information Coordinator will:

i. Notify the Information Privacy Commissioner (IPC);
ii. Notify individuals or determine an exemption applies; and
iii. Make other notifications as required which could include:
   - NSW Police Force and/or Australian Federal Police, where CN suspects a data breach is a result of criminal activity
   - Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, 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 the 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.

iv. Individuals/organisations affected by an Eligible Data Breach will generally be notified as soon as practicable or within 5 days and CN may issue a public notification on its website.

v. CN will implement guidance from the IPC.

e) Step five: Review

CN will undertake an After Action Review in accordance with its CEMP for all Eligible Data Breaches to determine root causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

The outcome of an After Action Review could include:

i. review of IT systems and remedial actions to prevent future data breaches
ii. security audit of security controls
iii. review of policies and procedures
iv. review of training
v. review of contractual obligations

The After Action Review will assign responsibilities for agreed actions and an overview of the incident and After Action Review will be reported to CN's Audit and Risk Committee.

Part C Roles and Responsibilities

10 Executive Director, Corporate Services

The Executive Director Corporate Services is responsible for:

10.1 oversight of this Policy;

10.2 undertaking activation protocol of the CEMP;

10.3 reporting data breaches to the CEO;

10.4 seeking approval from the CEO about public communications;

10.5 reviewing and determining a recommendation from the Privacy & Information Coordinator as to whether the data breach in Eligible Data Breach; and

10.6 oversight of all notifications and actions for Eligible Data Breaches.

11 Chief Information Officer

The Chief Information Officer is responsible for:

11.1 having an approved Cyber Security Incident Plan in place to manage CN's data breach response, integrated with business continuity arrangements;

11.2 immediately notifying the Cyber Incident Response Team;

11.3 investigating the data breach and completing a Data Breach Report and Action Plan (where the breach involves an IT system); and

11.4 liaising with the Executive Manager Media Engagement Economy & Corporate Affairs to determine a strategy for public communication.

12 Executive Manager, Media Engagement Economy & Corporate Affairs (MEECA)

The Executive Manager, MEECA is responsible for:

12.1 providing advice on the public communication strategy and messaging to affected external individuals.

13 Privacy & Information Coordinator

The Privacy & Information Coordinator is responsible for:

13.1 preparing advice for the Executive Director Corporate Services as to whether the data breach is an Eligible Data Breach for external notification;

13.2 liaising with the Executive Manager Media Engagement Economy & Corporate Affairs to determine a strategy for public communication;

13.3 reporting the Eligible Data Breach to the IPC;

13.4 investigating the data breach completing a Data Breach Report and Action Plan (where the breach involves hard copy records);

13.5 maintaining the internal and public registers for Eligible Data Breaches.

14 All CN Staff

14.1 All CN Staff have a responsibility to immediately report a suspected data breach in accordance with this Policy.

ANNEXURE A - DEFINITIONS

CEO means Chief Executive Officer of the City of Newcastle and includes their delegate or authorised representative.

References to the Chief Executive Officer are references to the General Manager appointed under the *Local Government Act 1993* (NSW).

City of Newcastle (CN) means Newcastle City Council.

CN Staff means employees of CN (including full time, part time, fixed term and casual) or Specific Talent Contractor who is engaged under a CN position description.

Council means the elected Council.

Councillor means a person elected to civic office as a member of the governing body including the Lord Mayor.

Unless stated otherwise, a reference to a section or clause is a reference to a section or clause of this Policy.

Eligible Data Breach means breaches described in section 5.3 of this Policy.

Personal Information means '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). That is 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.

ANNEXURE B - POLICY AUTHORISATIONS

In accordance with section 378 of the Local Government Act 1993, the Chief Executive Officer delegates the following functions to the positions listed:

Title of authorisation	Description of authorisation	Position Number and Title
Nil	Nil	Nil

DOCUMENT CONTROL

Policy title	Data Breach Policy
Policy owner	Executive Manager Legal & Governance
Policy expert/writer	Privacy & Information Coordinator
Associated Procedure Title	Cyber Incident Response Plan (CIRP)
Guideline or Procedure owner	Executive Manager Legal & Governance
Prepared by	Legal & Governance
Approved by	CEO
Date approved	4/12/2023
Commencement Date	4/12/2023
Next review date	30/04/2026
Termination date	30/04/2027
Version #	Version number 1
Category	Privacy and Access to Information
Details of previous versions	NIL
Keywords	Cyber, security, information, technology, data, breach, privacy, personal information
Relevant Newcastle 2040 Theme/s	Liveable
Relevant legislation/codes (reference specific sections)	This Policy supports CN's compliance with the following legislation: • *Privacy and Personal Information Protection Act 1998* • *Health Records and Information Protection Act 2002* • *Government Information (Public Access) Act 2009* • *State Records Act 1998*
Other related documents	CN Cyber Security Strategy 2023-2026 2040 Community Strategic Plan Cyber Security Policy Cyber Security Management Plan 2020 Privacy Management Plan Records Management Policy Data Breach Report and Action Plan
Related forms	NIL
Required on website	Yes
Authorisations	Functions authorised under this Policy at Annexure B