Data Breach Policy

Date Adopted: Tuesday, 26 November 2024

Version: 1.1

Policy Objectives

Maitland City Council recognises the importance of protecting personal information and is committed to ensuring the confidentiality, integrity, and security of the personal information held by Council.

Council operates in compliance with mandatory notification provisions under Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act'), also referred to as the Mandatory Notification of Data Breach ('MNDB') Scheme.

This policy sets out how Council will respond to a data breach.

Policy Scope

This Policy applies to all Council staff, councillors, contractors, volunteers, vendors, authorised users of Council's Information and Communication Technology ('ICT') systems, networks, software, or hardware, and any other third party who collects or manages personal information on behalf of Council.

Policy Statement

Mandatory notification of data breach scheme

Under the PPIP Act all public sector agencies, including local councils, are to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Under the MNDB Scheme Council has an obligation to:

- immediately make all reasonable efforts to contain a data breach.
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach.
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach.
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach.
- notify the Privacy Commissioner and affected individuals of the eligible data breach.
- comply with other data management requirements, including a publicly accessible data breach policy, a public register of data breach notifications issued by Council, and an internal register of eligible data breaches.

What is a data breach?

A data breach occurs when personal 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.

This may or may not involve disclosure of personal information external to Council or publicly. For example, unauthorised access to personal information by a Council staff member, or unauthorised sharing of personal information to the public or between teams within Council may constitute 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 when a data breach may occur include:

- When a letter or email containing personal information is sent to the wrong recipient.
- When a physical asset like a laptop or USB stick containing personal information is lost, misplaced, or stolen.
- Cyber incidents such as ransomware, malware, hacking or phishing.
- Where a coding error allows access to a system without authentication.
- Insider threats from employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

Reporting a suspected data breach

Any Council staff member, councillor, contractor, volunteer, third party, or member of the public with reasonable grounds to suspect that a data breach has occurred should immediately report the suspected breach to Council's Privacy Officer (privacy@maitland.nsw.gov.au), providing as much information as they can about the suspected data breach, including type of personal information involved, date and time the breach occurred, location of data or equipment affected, and whether the loss puts any person or other data at risk.

Managing data breaches

Data Breach Response Plan

Council has established a Data Breach Response Plan that documents the process that Council will take to respond to a reported data breach. The Data Breach Response Plan is included in the Privacy Management Plan.

The Data Breach Response Plan comprises of the following steps:

Initial report and triage

An initial assessment of the reported data breach will be undertaken to determine the type and sensitivity of personal information involved, the persons to whom the personal information was exposed, the risk of harm to the individuals involved and the nature of any potential harm, and whether it may be necessary to convene a Data Breach Response Team.

Contain

Council will immediately make all reasonable efforts to contain the breach as soon as possible to prevent any further compromise of personal information and minimise harm to affected individuals.

Assess and mitigate

An assessment of the data breach will be undertaken to determine the cause of the data breach, understand the risk of harm to affected individuals, and identify and take all appropriate actions to limit the impact of the data breach.

An assessment must be carried out within 30 days after a suspected data breach is reported to determine whether there are reasonable grounds to believe that the suspected data breach is an eligible data breach.

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.

Notify

Council must notify the NSW Privacy Commissioner and affected individuals of eligible data breaches.

Once it is determined that an eligible data breach has occurred, the NSW Privacy Commissioner must be immediately notified in the approved form, with a follow up notification provided of any information that was not included in the initial notification. Affected individuals must be notified as soon as practicable. If we are unable to directly notify any or all affected individuals, we will issue and publish a public notification.

Review

Following a data breach, a post incident review will be undertaken to identify and remediate any processes or weaknesses in information security and data handling that may have contributed to the data breach to prevent future breaches, and to assess the effectiveness of this policy and the data breach response process.

Record-keeping

Council will maintain appropriate records to provide evidence of how all data breaches are managed.

Council will establish and maintain an internal register of eligible data breaches.

Council will maintain and publish on our website a public notification register of any public data breach notifications that we have issued.

Training and awareness

Council will provide regular training to Council staff and contractors on the importance of safeguarding personal information, how to identify and report a suspected data breach, and the data breach response process.

Accessibility of this policy

This policy will be made publicly available on Council's website as well as the staff intranet.

Review and Testing

This policy will be reviewed, tested, and updated on an annual basis.

Roles and Responsibilities

General Manager

The General Manager is responsible for:

- Ensuring that Council is compliant with all relevant laws and regulations.
- Determining whether a Data Breach Response Team is to be convened and selecting the members of the Data Breach Response Team.
- Approving an extension of time to conduct the assessment of a suspected data breach.
- Determining whether the data breach is eligible for external notification.
- Undertaking external notifications to the NSW Privacy Commissioner and affected individuals/organisations.
- Notifying the NSW Privacy Commissioner of any further information and when an extension of time to the assessment period has been approved.
- Notifying Council's insurers as required.

Executive Manager Customer and Digital Services

- Having an approved Data Breach Policy and Data Breach Response Plan in place to manage Council's data breach response.
- Taking action to respond to the actual or suspected data breach in accordance with the Data Breach Response Plan.
- Implementing any longer terms actions to contain and response to security threats to Council's ICT systems and infrastructure.

Privacy Officer

The Manager Enterprise Architecture is Council's Privacy Officer.

The Privacy Officer is responsible for:

- Receiving and assessing reports of actual or suspected data breaches.
- Initiating the Data Breach Response Plan.
- Preparing an initial data breach assessment report, including advice for the General Manager to determine if a Data Breach Response Plan is to be convened.
- Investigating and managing Council's response to a data breach where it is determined that a Data Breach Response Team is not necessary.
- Reviewing and updating the Data Breach Policy and Data Breach Response Plan.
- Planning, initiating, overseeing, and reporting on the testing of this policy and the Data Breach Response Plan.

Data Breach Response Team

The Data Breach Response Team is responsible for:

- Assembling promptly to investigate and manage Council's response to a data breach in accordance with the Data Breach Response Plan.
- Preparing advice for the General Manager to determine if the data breach is eligible for external notification.

Vendors/Third Parties

Vendors/Third Parties are responsible for:

- Immediately notifying Council of any actual or suspected data breaches affecting Council.
- Having appropriate security measures in place to protect any personal information it collects or manages on behalf of Council.

All staff

All Council staff, councillors, contractors, and volunteers are responsible for:

- Immediately reporting any actual or suspected data breaches to the Privacy Officer.
- Undertaking required training relating to privacy, PPIP Act requirements, and Council's data breach response process.
- Complying with this policy.

Members of the Public

Members of the public outside of Council can report an actual or suspected data breach affecting Council.

Policy Definitions

Affected individual	As defined in section 59D of the PPIP Act, an affected individual is an individual: • to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and • who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.
Data breach	Data breach means unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information. Examples of a data breach are when a device containing personal information is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.
Data Breach Response Team	Team of assessors assigned to investigate and manage Council's response to a data breach as outlined in the Data Breach Response Plan. The General Manager will determine if a Data Breach Response Team is to be convened and select the members of the Data Breach Response Team. A member of the Data Breach Response Team may be: • An officer or employee of Maitland City Council, or

- An officer or employee of another public sector agency acting on behalf of Maitland City Council, or
- A person acting on behalf of Maitland City Council, or a person employed by that person (e.g., an individual employed by a third party to carry out the assessment for Maitland City Council).
- To the exclusion of any person the General Manager reasonably suspects was involved in an act or omission that led to the data breach.

Eligible data breach

As defined in section 59D of the PPIP Act, an eligible data breach means:

(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency 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, or

(b) personal information held by a public sector agency is lost in circumstances where—

(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

(ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

Health information

A specific type of personal information which may include information or an opinion about the physical or mental health or a disability (at any time) of an individual. This includes, for example, information contained in medical certificates, information about medical appointments or test results.

Loss

Loss refers to the accidental or inadvertent loss of personal information held by Council, in circumstances where is it is likely to result in unauthorised access or disclosure. For example, where a staff member leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

Personal information

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 could be reasonably ascertained from the information or opinion, as defined in section 4 of the PPIP Act.

For the purpose of this policy, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.

Public data breach notification	Notification made to the public at large rather than a direct notification to an identified individual.
Serious harm	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 affected individual. That is, 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 Council's position would identify as a possible outcome of the data breach.
Unauthorised access	Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, a staff member browses a fellow employee's personnel record without any legitimate purpose.
Unauthorised disclosure	Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted by the PPIP Act. This includes an unauthorised disclosure by an employee of the organisation. For example, a staff member accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.

Policy Administration

BUSINESS GROUP:	Customer and Digital Services
RESPONSIBLE OFFICER:	Executive Manager Customer and Digital Services
COUNCIL REFERENCE:	
POLICY REVIEW DATE:	Three (3) year from date of adoption
FILE NUMBER:	35/1
RELEVANT LEGISLATION	Health Records and Information Protection Act 2002 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) Privacy and Personal Information Protection Amendment Bill 2022 (NSW) Privacy and Personal information Protection Regulation 2019 (NSW) State Records Act 1998 (NSW)
RELATED POLICIES / PROCEDURES / PROTOCOLS	Privacy Management Plan Privacy Policy Records Management Policy Cyber Information Security Policy

Policy History

VERSION	DATE APPROVED	DESCRIPTION OF CHANGES
1.0	24/10/2023	New policy to comply with the mandatory notification provisions under Part 6A of the PPIP Act
1.1	TBC	Amended roles and responsibilities to be aligned to new MCC structure and Customer and Digital Services functions, added privacy email address. New Branding.