Council Policy

Data Breach

Version 2

29 September 2025

02 4921 0333 | COUNCIL@LAKEMAC.NSW.GOV.AU

126-138 MAIN ROAD SPEERS POINT NSW 2284 | BOX 1906 HUNTER REGION MAIL CENTRE NSW 2310

LAKEMAC.COM.AU

Introduction

Purpose

The purpose of this policy is to establish a comprehensive framework for Lake Macquarie City Council (Council) to effectively identify, manage, and respond to data breaches involving personal information, as required by the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

Scope

This policy outlines the principles and objectives which will guide Council in managing and responding to the risks of a data breach. This policy complies with section 59ZD of the PPIP Act. It provides a framework for Council's compliance with the Mandatory Notification of Data Breach Scheme (the MNDB Scheme).

This policy establishes responsibility and accountability for all steps in the process of addressing information security incidents that result in data breaches and describes clear roles and responsibilities with the aim of ensuring a comprehensive and well-managed privacy and information governance program.

This policy applies to:

- All staff, contractors, work experience and volunteers authorised to access Council information systems
- Consultants or organisations authorised to administer, develop, manage and support Council information and systems
- Third party suppliers, vendors, and contractors.

Policy statement

At Lake Macquarie City Council, we are committed to safeguarding the privacy and security of personal information entrusted to us by our customers, employees, and stakeholders.

Council will take reasonable steps to ensure that data and information collected is relevant, required and not excessive.

This Data Breach Policy outlines our approach in the event of a data breach to ensure a swift, transparent, and effective response.

What is a data breach?

A data breach occurs when there is an unauthorised access to, or unauthorised disclosure of, personal information, or there is a loss of personal information in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

Reporting a Data Breach

All actual or suspected Data Breaches are to be reported immediately to Council's Privacy Officer. The Privacy Officer will undertake a swift and thorough assessment of the breach to determine its scope, potential harm and legal obligations.

Responding to a Data Breach

- **Data Breach Response Plan:** Council maintains a framework which sets out roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken in managing a breach if one occurs. It provides decision-making tools and guidance to assist Council to respond to actual or suspected eligible data breaches.
- **Containment:** immediate steps are taken to contain the breach, limit further unauthorised access or disclosure, and mitigate potential harm.
- **Risk assessment:** risk assessments are conducted to determine the likelihood of serious harm to affected individuals.
- **Consider notification and activating Data Breach Response Team:** the outcome of risk assessments is used to consider notification to affected individuals and escalation to Council's Executive including activating the Data Breach Response Team. Data breaches are dealt with on a risk-based case-by-case basis, to inform the appropriate course of action.

  The Data Breach Response Plan is established by the Data Breach Response Team, which includes (but is not limited to) key representatives from Customer Experience, Information Technology (IT), Legal, Communications and Corporate Performance, and senior management, including:

  - Director Organisational Services
  - Chief Technology Officer
  - Coordinator Cyber Security
  - Manager Customer Experience
  - Privacy Officer
  - Manager Communications and Corporate Performance
  - Legal counsel
  - Depending on the nature of the breach, the Response Team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a representative from People and Culture.

  The Data Breach Response Team, in consultation with relevant Council data owners, will make recommendations to the CEO regarding notification to individuals who have been impacted in the data breach considering the following factors:
  - The risk of harm to the individual/organisation.
  - Steps that Council has taken to date to avoid or remedy any actual or potential harm.
  - The ability of the individual/organisation to take further steps to avoid or remedy harm.
  - Whether the information that has been compromised is sensitive, or likely to cause humiliation or embarrassment for the individual/organisation.
  - Whether there are any applicable legislative provisions or contractual obligations that require Council to notify affected individuals.

  The CEO considers the recommendations of the Data Breach Response team and is responsible for deciding whether the breach is a notifiable incident.

- **Review and response improvement:** a thorough review of the data breach incident is conducted to identify areas for improvement and where possible prevent reoccurrence.

Regular training and awareness programs are provided for staff to ensure a strong culture of privacy and data security are implemented. Council's review and response improvement process involves assessing the effectiveness of the policy (and making amendments as required) and strategies for identifying and remediating processes in handling data.

- **Record keeping:** a public notification register for any notifications given under section 59N(2) of the *PPIP Act* is published on Council's website and all records that provide evidence of how suspected breaches are managed, including those not escalated to the response team, are retained in Council's Electronic Document Records Management System and held in accordance with Council's Privacy Management Plan.

1. **Prevention and mitigation:** appropriate security measures are implemented, such as firewalls, encryption, access controls, and staff training, to safeguard personal and sensitive information. Security systems and processes are regularly reviewed and updated to ensure their effectiveness and compliance with relevant privacy laws and regulations.
2. **Early detection:** The policy aims to ensure early detection of data breaches, enabling the organisation to respond swiftly and minimise potential harm. Proactive monitoring and incident detection mechanisms are in place to identify suspicious activities or security incidents promptly.
3. **Timely response:** The data breach policy seeks to establish a well-defined and coordinated response to data breaches. The objective is to respond promptly and effectively to contain the breach, assess the impact, and implement appropriate mitigation measures.
4. **Minimise impact:** In the event of a data breach, the policy aims to minimise the impact on affected individuals and the organisation. By promptly identifying and addressing the breach, the goal is to limit the potential harm caused by the unauthorised access or disclosure of sensitive information.
5. **Compliance with legal requirements:** The policy objectives include ensuring compliance with relevant data protection laws, regulations, and industry standards. By adhering to applicable laws, such as the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Act 2002* and the *Privacy Act 1988*, the organisation demonstrates its commitment to legal and regulatory obligations.
6. **Transparency, accountability and external engagement:** The data breach policy seeks to promote transparency and accountability in the organisation's data breach response. Clear communication with affected individuals, regulatory authorities, and other stakeholders will be established to keep them informed about the breach and the steps taken to address it. This could include NSW Police Force, Cyber Security NSW, Australian Taxation Office, the Office of the Australian Information Commissioner, Australian Federal Police and the NSW Information and Privacy Commission.
7. **Continuous improvement:** The policy aims to facilitate a culture of continuous improvement in data breach prevention and response. Post-incident reviews and

assessments are conducted to identify areas for enhancement, refine response procedures, and strengthen overall data protection measures.

8. **Staff awareness and training:** The objective is to raise awareness among employees and relevant personnel about data breach risks and their roles in preventing and responding to incidents. Regular training is conducted to equip staff with the knowledge and skills necessary to safeguard personal and sensitive information.
9. **Vendor and third-party management:** The policy objectives include establishing robust vendor and third-party risk management practices. Ensuring that external partners are clear on their role in supporting Council to respond to data breach and that it is documented in legally binding contracts or memorandums of understanding.
10. **Ethical considerations:** The policy seeks to uphold ethical considerations in data handling, ensuring that individuals' rights and dignity are respected throughout the data breach response process. Personal information will be used ethically and lawfully for authorised purposes.
11. **Preparedness:** The policy aims to ensure the organisation's readiness to respond to data breaches effectively. Regular drills and exercises will be conducted to test response capabilities, identify gaps, and enhance preparedness.

By adhering to these objectives, the organisation demonstrates its commitment to safeguarding personal and sensitive information, maintaining regulatory compliance, and fostering a culture of privacy and data protection.

Review and evaluation

This Data Breach Policy will be reviewed every two years or as required to ensure its ongoing relevance, effectiveness, and compliance with applicable laws and regulations.

Controlled Document Information

Authorisation Details

Folder No:	F2023/02330	**TRIM Record No:**	D12157466
Audience:	External - All Council staff and customers		
Department:	Customer Experience	**Officer:**	Head of Customer Experience – Jasmyne Munro
Key focus area(s):	Governance		
Review Timeframe: **Max < 4 years**	2 years	**Next Scheduled Review Date:**	November 2027
Authorisation:	CEO and Council's Executive team – 29 September 2025		
Authorisation - Council Adoption Date:	Council Information Report – 23 February 2026		

Related Document Information, Standards & References

Related Legislation:	Privacy and Personal Information Protection Act 1998 (NSW) Health Records and Information Privacy Act 2002 (NSW) Privacy Act 1988	Legislation Legislation Legislation
Related Policies:	Privacy Management Plan Records Management Policy Enterprise Risk Management Framework Risk Appetite Statement	Outlines Council's Privacy Management Principles Outlines how Council stores, retains, and disposes of records and information.
Related Procedures, Guidelines, Forms, WHS Modules/PCD's, Risk Assessments, Work Method Statements:	Data Breach Response Plan	Outlines the steps taken in the event of a data breach or suspected data breach.
Standards, COP's & Other References	(Standard, COP or Other References)	(Relationship/Context)

Definitions

Term / Abbreviation	Definition
Data breach	An incident where there has been unauthorised access to, disclosure of, or loss of personal or sensitive information, which poses a risk of harm to the affected individuals.
Personal information	Information or an opinion about an identified or identifiable individual.
Public Notification	A notification provided under s59N(2) of the PPIP Act when any or all of the individuals affected by an Eligible Data Breach are unable to be notified individually. Public Notifications are maintained in a Register on Council's website
Sensitive information	Personal information that includes details such as race, religion, sexual orientation, health information, biometric data, financial information, etc

Notifiable Data Breach	A data breach that meets the criteria specified in Council's Data Breach Response Plan and requires notification to affected individuals and relevant agencies such as the NSW Information and Privacy Commission.

Consultation (update for each version created)

Key Departments, Teams, Positions, Meetings:	Legal, Internal Ombudsman, Privacy Officer, Governance and Privacy Lead, Organisational Leadership Team

Version History

Version No	Date Changed	Modified By	Details and Comments
1	24 July 2023	J Munro	Created policy
2	04/09/2025	J Munro	Updated policy to include a definition of a data breach and information on record keeping.