LAKE MACQUARIE CITY

Council Policy

Data Breach

Version 1 - 31 October 2023

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). This policy aims to ensure the protection of individuals' privacy under Council's Privacy Management Plan and uphold the organisation's commitment to safeguarding the confidentiality, integrity, and availability of data.

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 is designed to comply with the *Privacy and Personal Information Protection Act 1998,* the *Health Records and Information Privacy Act 2002* and the Australian Privacy Principles (APPs) outlined in the *Privacy Act 1988*.

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.

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.

Principles

The following principles are applied through this policy:

- **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.
- **Data Breach Response Plan:** 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 will also provide decision-making tools and guidance to assist Council to respond to actual or suspected eligible data breaches.
- **Breach identification and assessment:** Council has mechanisms for proactive monitoring and detection of data breaches including technical controls and monitoring services, audits and reviews. In the event of a suspected or identified data breach, the Privacy Officer is immediately notified. A swift and thorough assessment of the breach to determine its scope, potential harm, and legal obligations is conducted.

- **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 are 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, Business Information and Technical Solutions (BITS), Legal, Communications and Corporate Strategy, and senior management, including:
  - Director Organisational Services
  - Chief Information Officer
  - Group Leader Technology and Cyber Security
  - Head of Customer Experience
  - Privacy Officer
  - Head of Communications and Corporate Strategy
  - 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 regarding notification of 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.
- **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.

How Council will respond to data breaches

1. **Prevention:** The primary objective of the Data Breach policy is to prevent data breaches from occurring in the first place. By implementing robust information security measures, the organisation aims to reduce the risk of unauthorised access, disclosure, or loss of personal and sensitive information.

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 and accountability:** 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 and the 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 will 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.

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:**	D11086518
Audience:	External - All Council staff and customers		
Department:	Customer Experience	**Officer:**	Head of Customer Experience – Jasmyne Munro
Key focus area(s):	Shared Decision Making		
Review Timeframe: **Max < 4 years**	2 years	**Next Scheduled Review Date:**	31 October 2025
Authorisation:	Endorsed by the CEO - 31 October 2023		
Authorisation - Council Adoption Date:	Noted by Council - 27 November 2023		

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 Policy and Framework	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.
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 our 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