POLICY:-	
Policy Title:	Data Breach Policy
File Reference:	F10/618-013
Date Policy was adopted by Council initially:	14 December 2023
Resolution Number:	250/23
Other Review Dates:	
Resolution Number:	
Current Policy adopted by Council:	14 December 2023
Resolution Number:	250/23
Next Policy Review Date:	2026
PROCEDURES/GUIDELINES:-	
Date procedure/guideline was developed:	N/A
Procedure/guideline reference number:	N/A
RESPONSIBILITY:-	
Draft Policy developed by:	Manager IT/GIS Manager Governance
Committee/s (if any) consulted in the development of this Policy:	N/A
Responsibility for implementation:	Manager IT/GIS Director of Environment and Planning
Responsibility for review of Policy:	Manager IT/GIS

1. Introduction

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 every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches. Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

This policy outlines Upper Lachlan Shire Council's approach to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

2. Scope

This policy applies to all staff and contractors of Upper Lachlan Shire Council. This includes temporary and casual staff, private contractors and consultants engaged by Upper Lachlan Shire Council to perform the role of a public official. This policy also applies to third party providers, who hold personal and health information on behalf of Upper Lachlan Shire Council.

This policy should be reviewed at regular intervals or where improvements are identified in response to a data breach, whichever occurs sooner.

3. Purpose

This policy sets out how Upper Lachlan Shire Council will respond to data breaches involving personal information. Upper Lachlan Shire Council acknowledges that not all data breaches will be eligible data breaches but regardless, Upper Lachlan Shire Council takes all data breaches seriously. The policy details:-

- What constitutes an eligible data breach under the PPIP Act;
- Roles and responsibilities for reporting, reviewing and managing data breaches;
- The steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

Effective breach management, including notifications, assists Upper Lachlan Shire Council in avoiding or reducing possible harm to both the affected individuals/organisations and Upper Lachlan Shire Council, and may prevent future breaches.

4. Roles and Responsibilities

The following staff have identified roles under the Data Breach Policy:-

- Council Chief Executive Officer and Department Directors/Executive Management (MANEX) – responsible for ensuring development of a Data Breach Policy, development of internal register and Public Notification Register for data breaches and are responsible for reporting data breaches to Manager IT/GIS.
- Manager IT/GIS - responsible for implementing this Policy, reporting data breaches to the Chief Executive Officer and MANEX and all notifications and actions for eligible data breaches to external agencies. Implementing and updating the internal register and Public Notification Register.
- Information Systems Coordinator / IT Systems Support Officer - responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches.
- Communications Officer – responsible for provision of advice on the

communication strategy and messaging to affected individuals and external reporting agencies.

- Upper Lachlan Shire Council employees - all employees have a responsibility for immediately reporting a suspected data breach in accordance with this Policy.

All Council staff, Councillors, contractors, consultants, volunteers and members of Section 355 Committees of Council have a responsibility to notify the Manager IT/GIS of any data breaches as soon as they become aware that a data breach has occurred and provide information about circumstances and incidence relating to the data breach.

5. What is an eligible data breach?

The definition of personal information for the purposes of the MNDB Scheme includes both '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). This means that for the purposes of the MNDB Scheme, 'personal information' means *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.

A data breach occurs when personal information held by an agency (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 the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to 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 data breaches include:-

- **Human error**
    - When a letter or email is sent to the wrong recipient.
    - When system access is incorrectly granted to someone without appropriate authorisation.
    - When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
    - When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
- **System failure**
    - Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
    - Where systems are not maintained through the application of known and supported patches.
- **Malicious or criminal attack**
    - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.

- Social engineering or impersonation leading into inappropriate disclosure of personal information.
- Insider threats from agency employees 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.

The MNDB Scheme applies where an 'eligible data breach' has occurred. 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.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:-

- The type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk;
- The level of sensitivity of the personal information accessed, disclosed or lost;
- 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;
- 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);
- The circumstances in which the breach occurred; and
- Actions taken by the agency to reduce the risk of harm following the breach.

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.

6. Systems and Processes for Managing Data Breaches

Upper Lachlan Shire Council has established a range of systems and processes for preventing and managing data breaches, including a number of cyber security measures to mitigate the risk of data breaches. This has included projects to increase cyber security maturity and provide cyber security training for all staff.

Council will ensure all third-party providers who store personal and health information on behalf of Upper Lachlan Shire Council, are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches to Upper Lachlan Shire Council.

Council has included the risk of a cyber-security incident (which may involve a data breach) within its Risk Register and established controls to mitigate this risk and its impact on Upper Lachlan Shire Council's systems through subsequent procedures. The loss of IT systems as a result of a cyber-security incident is to be included in Upper Lachlan Shire Council's Business Continuity Plan.

Related Legislation and Council Policies

- Privacy and Personal Information Protection Act 1998;
- Ombudsman Act 1974;
- Health Records and Information Privacy Act 2002;
- State Records Act 1998;
- Government Information (Public Access) Act 2009;
- Local Government Act 1993;
- Independent Commission against Corruption Act 1988;
- Work Health and Safety Act 2011;
- Public Interest Disclosures Act 1994;
- IPC Data Breach Self-assessment Tool for Mandatory Notification of Data Breach
- Code of Conduct;
- Information Technology Strategic Plan;
- Digital Information Security Policy;
- Complaints Management Policy;
- Records Management Policy;
- Internal Audit and Risk Management Policy;
- Government Information (Public Access) Policy;
- Fraud and Corruption Prevention Policy;
- Gathering Information Policy;
- Business Continuity Plan.

Variation

Council reserves the right to vary or revoke this Policy.