Data Breach Policy

Document Authorisation and Control

RESPONSIBLE OFFICER:	Manager Governance, Risk and Corporate Planning (MGRCP)				
REVIEWED BY:	Management Executive Team (Manex)				
REVIEW DUE DATE:	December 2026				
VERSION NUMBER:	1				
VERSIONS:	**DATE:**	**RESOLUTION NO:**	**DESCRIPTION OF AMENDMENTS:**	**AUTHOR / EDITOR:**	**APPROVED / ADOPTED BY:**
1	21/12/2023	8.12/23	The creation of the Policy.	MGRCP	Council

…….
General Manager

21/12/23

…….
Date

Acknowledgement of Country

Glen Innes Severn Council (Council) acknowledges and pays respect to the Ngarabul people as the traditional custodians of this land, their elders past, present and emerging and to Torres Strait Islander people and all First Nations people.

1. Preliminary

Purpose

The purpose of this policy is to set out requirements of the mandatory notifiable data breach scheme that applies under the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

Applicability

This policy applies to all Council employees.

Outcomes

The main objectives of this policy are to:

1. Provide guidance for responding to a breach of information held by Council.

2. Provide considerations around notifying persons whose privacy may be affected by the breach.

3. Assist Council in avoiding or reducing possible harm to both the affected individuals / organisations and Council.

4. Prevent future breaches.

2. Policy Statement

This policy outlines Council's overall strategy for managing data breaches from start to finish.

Council is committed to:

- preparing for, evaluating, responding to and reporting on data breaches at the appropriate level and in a timely fashion,
- mitigating potential harm to affected individuals and Council itself, and
- meeting the compliance obligations under the PPIP Act.

This Policy will be published on Council's website.

3. Introduction

Background and Terminology

1. What is an eligible data breach?

An 'eligible data breach' occurs where:

1. There is an unauthorised access (whether deliberate or accidental) to, or unauthorised disclosure of, personal information held by Council or there is a loss of personal information held by Council 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.

2. What is the Mandatory Notification of Data Breach (MNDB) scheme?

Mandatory Notification of Data Breach (MNDB) scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

The scheme also applies to 'health information,' defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, Council is not required to notify individuals or the Commissioner but should still take action to respond to the breach. Council may still provide voluntary notification to individuals where appropriate.

4. Procedure

The PPIP Act creates an MNDB scheme which requires public sector agencies, including councils, to notify the NSW Information and Privacy Commission (IPC) and affected individuals of data breaches involving personal or health information likely to result in serious harm. Therefore, not all data breaches are notifiable.

1. Any suspected data breach, whether accidental or deliberate, whether carried out by internal or external actors must be reported immediately to the Privacy Contact Officer.

2. If, after an initial investigation, the Privacy Contact Officer suspects a notifiable data breach may have occurred, a reasonable and expeditious assessment must be undertaken to determine if the data breach is likely to result in serious harm to any individual affected.

3. Council's Privacy Contact Officer will seek information to assess the suspected breach.

4. In assessing a suspected breach, the Privacy Contact Officer may require assistance and information from other areas of the Council depending on the

circumstances. In this regard, the Privacy Contact Officer will consult Council's Data Breach Readiness Solution.

5. There will then be an evaluation of the scope and possible impact of the breach.

6. The Privacy Contact Officer will assess if a breach is likely to be notifiable and ensure appropriate actions, including reporting to the IPC.

7. An assessment of a known or suspected breach must be conducted expeditiously and where possible, should be completed within 30 days.

8. In all cases, the assessment will identify what actions must be taken including:

    - how to contain or minimise possible damage,
    - notification requirements and to whom, and
    - post incident review and preventative efforts.

9. These actions will be documented and acted upon as soon as possible.

10. A breach, which is assessed as likely to result in serious harm to individuals whose personal information is involved, is a notifiable data breach. Such data breaches must be notified to the affected individuals and the IPC.

11. Notice will include information about the breach and the steps taken in response to the breach.

Note: If Council has responded quickly to the breach, and because of this action the data breach is not likely to result in serious harm, then the individuals and the IPC will not usually be contacted. However, Council staff may decide to advise the affected individuals about the incident for the sake of transparency.

The risk of serious harm will be assessed by considering both the *likelihood* of the harm occurring and the *consequences* of the harm.

Some of the factors that will be considered are:

Factors	Considerations
The type of personal information involved in the data breach.	Some kinds of personal information are more sensitive than others and could lead to serious ramifications for individuals if accessed. Information about a person's health, documents commonly used for identity fraud (e.g., Medicare card, driver's licence) or financial information are examples of information that could be misused if the information falls into the wrong hands.

Factors	Considerations
Circumstances of the data breach	The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to many individuals would normally lead to an overall increased risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant. Consideration must be given to who may have gained unauthorised access to information, and what their intention was (if any) in obtaining such access. It may be that there was a specific intention to use the information in a negative or malicious way.
Nature of possible harm	Consider the broad range of potential harm that could follow from a data breach including: • identity theft, • financial loss, • threat to a person's safety, • loss of business or employment opportunities, and • damage to reputation (personal and professional).

5. Roles and Responsibilities

The Privacy Contact Officer, as appointed under Council's Privacy Management Plan (the Manager Governance, Risk and Corporate Planning), will coordinate the assessment of a suspected data breach in accordance with this Policy and ensure the requirements under the PPIP Act are met.

Notification to the IPC and internally within Council is the responsibility of the Privacy Contact Officer.

Notification to individuals may be undertaken by the Privacy Contact Officer or a Council officer in the area in which the breach occurred after the Privacy Contact Officer agrees to the action.

The Privacy Contact Officer will consult Council's Data Breach Readiness Solution and involve the core crisis team as and when necessary.

6. Legislation And Supporting Documents

Relevant Legislation, Regulations and Industry Standards include:

- *Privacy and Personal Information Protection Act 1998*

- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Regulation 2019*
- *NSW Government Information Classification, Labelling and Handling Guidelines (July 2015)*

Relevant Council Policies and Procedures include:

- Privacy Management Plan,
- Business Continuity Plan,
- ICT Policy and Procedures,
- Data Breach Readiness Solution, and
- Records Management Policy.

7. Variation And Review

The Data Breach Policy will be reviewed every term of Council, or earlier if deemed necessary, to ensure that it meets the requirements of legislation and the needs of Council. The term of the Policy does not expire on the review date, but will continue in force until superseded, rescinded or varied either by legislation or a new resolution of Council.