DATA BREACH RESPONSE COUNCIL POLICY

ADOPTED BY COUNCIL: 9 OCTOBER 2023

PURPOSE

To set out requirements of the mandatory notifiable data breaches scheme that applies under the *Privacy and Personal Information Protection Act 1998 (PPIP Act).*

POLICY INTENT

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 and may prevent future breaches.

WOLLONGONG 2032 OBJECTIVES

This policy aligns to Goal 4 of our Community Strategic Plan, "We are a connected and engaged community. This policy relates to strategies, 4.2, Improve digital access and participation across communities, 4.8 Council's resources are managed effectively to ensure long term financial sustainability and, 4.12 Technology is used to enhance urban planning and service provision for our community.

POLICY

The PPIP Act creates a Mandatory Notification of Data Breaches (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.

Not all data breaches are notifiable. If, after an initial investigation, the Privacy 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.

Council's Privacy Officer will seek information to assess the suspected breach. In assessing a suspected breach, the Privacy Officer may require assistance and information from other areas of the Council depending on the circumstances.

There will then be an evaluation of the scope and possible impact of the breach. The Privacy Officer will assess if a breach is likely to be notifiable and ensure appropriate actions including reporting to the IPC. An assessment of a known or suspected breach must be conducted expeditiously and where possible should be completed within 30 days.

In all cases the assessment will identify what actions must be taken. These will be documented and acted upon as soon as possible.

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

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.
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 a large number of 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).

LEGISLATIVE REQUIREMENTS

Privacy and Personal Information Protection Act 1998

NSW Privacy and Personal Information Protection Regulation 2019

NSW Government Information Classification, Labelling and Handling Guidelines (July 2015)

REVIEW

This Policy will be reviewed a minimum of once every term of Council, or more frequently as required.

REPORTING

Notification is only required under this policy in the event of a serious data breach. Notifications will follow any format and guidance issued by the NSW Information and Privacy Commission.

ROLES AND RESPONSIBILITIES

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

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

RELATED STRATEGIES, POLICIES AND PROCEDURES

Information Security Incident Response Management Policy

Cyber Security Incident Response Procedure

DEFINITIONS

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.

Notifiable data breach means a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner.

Personal information means information or an opinion about an individual who is identified, or who can reasonably be identified, from the information, whether or not the information or opinion is true or recorded in a material form, and includes sensitive information; and

Sensitive information means information or an opinion that is also personal information, about a person's racial or ethnic origin, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practises, criminal history, health information, and genetic and biometric information.

APPROVAL AND REVIEW	
Responsible Division	Information Management + Technology
Date adopted by Council	9 October 2023
Date/s of previous adoptions	NA
Date of next review	9 October 2026