DRAFT Data Breach Policy

MSC038E

Authorisation Details

Authorised by:		**Internal/External:**	External
Date:		**Minute No:**	
Review timeframe:	Every 4 years or in accordance with legislative changes.	**Review due date:**	
Department:	Office of the General Manager - Legal		
Document Owner:	Public Officer		
Community Strategic Plan Goal	6. Collaborative and responsive leadership that meets the expectations and anticipates the needs of the community		
Community Strategic Plan Strategy	6.2 Ensure Council is well managed, appropriately resourced, effective, efficient, accountable and responsive to its communities and stakeholders		
Delivery Program activity	6.2.1 Maintain a strong focus on financial discipline to enable Council to properly respond to the needs of the communities it serves		

Table of Contents

1. Policy Objective

In accordance with the *Privacy and Personal Information Protection Amendment Act 2022* (NSW) (the Amending Act) from 28 November 2023, the NSW mandatory data breach scheme will take effect under the *Privacy and Personal Information Protection Act 1998* (NSW) (the Act).

Under the mandatory data breach scheme public agencies must notify affected individuals and the Privacy Commissioner when a data breach is likely to result in serious harm to an individual whose personal information has been compromised.

In addition, the Amending Act requires Council to prepare and publish a data breach policy and establish and maintain an internal register for eligible data breaches.

The purpose of this policy is to facilitate Muswellbrook Shire Council's (Council) compliance with the amendments to the Act.

2. Risks being addressed

Council views the responsible handling of personal information to be a key cornerstone of sound corporate governance. Council is committed to full compliance with the obligations contained in the Act.

3. Scope

The scope of this policy applies to all data held by Council in either a paper based or electronic format and is applicable to all employees (including Councillors, contractors, students, volunteers and agency personnel) as well as external organisations and contractors who have been granted access to Council's infrastructure, services and data.

4. Policy Statement

Council governs the Muswellbrook Shire local government area by carrying out a variety of activities, functions and services to meet local community needs.

Council's functions are to be exercised by the following general principles prescribed in the *Local Government Act 1993* (NSW) (LG Act),:

a) Councils should provide strong and effective representation, leadership, planning and decision-making.

b) Councils should carry out functions in a way that provides the best possible value for residents and ratepayers.

c) Councils should plan strategically, using the integrated planning and reporting framework, for the provision of effective and efficient services and regulation to meet the diverse needs of the local community.

d) Councils should apply the integrated planning and reporting framework in carrying out their functions so as to achieve desired outcomes and continuous improvements.

e) Councils should work co-operatively with other councils and the State government to achieve desired outcomes for the local community.

f) Councils should manage lands and other assets so that current and future local community needs can be met in an affordable way.

g) Councils should work with others to secure appropriate services for local community needs.

h) Councils should act fairly, ethically and without bias in the interests of the local community.

i) Councils should be responsible employers and provide a consultative and supportive working environment for staff.

Council provides activities, functions and services including, but not limited to:

- arts and cultural programs;
- economic development;
- capital works and maintenance of Council assets and infrastructure (e.g. roads, footpaths, drainage, public spaces & community facilities);
- community health services;
- children and family services;
- customer service, governance and administration;
- local laws enforcement & regulation;
- waste & recycling management;
- management of parks, gardens, sportsgrounds and recreational spaces;
- financial planning, budgets, valuations, rates and credit control;
- environmental planning, stewardship and management programs;
- statutory planning and building regulation;
- community support and development;
- IT infrastructure;
- animal management;
- business and trade development;
- media, marketing and communications; and,
- strategic land use planning and heritage.

Depending on the circumstances and nature of your interaction with Council, the personal information Council typically collects includes, but is not limited to the following:

- name;
- address (residential, postal and/or email);
- telephone number (work, home or mobile);
- date of birth;
- signature;
- motor vehicle registration number; and/or,
- photograph and/or video footage.

Council must comply with the notification requirements relevant to an eligible data breach, as failure to do so may render Council liable for significant penalties.

4.1 What is an eligible data breach?

An eligible data breach is where:

(i) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and 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, or

(ii) personal information held by a public sector agency is lost in circumstances where:

(a) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

(b) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

To avoid doubt, an eligible data breach may include the following:

(i) a data breach that occurs within a public sector agency;

(ii) a data breach that occurs between public sector agencies;

(iii) a data breach that occurs by an external person or entity accessing, without authorisation, data held by a public sector agency.

4.2 Eligible data breach response process

Contain

If a Council officer is aware that there are reasonable grounds to suspect there may have been an eligible data breach of the Council, the Council officer will report the data breach to the General Manager.

If the General Manager receives a Council officer report regarding a suspected eligible data breach of the Council, the General Manager will immediately make all reasonable efforts to contain the data breach (this may involve coordinating with the other members or staff to ensure necessary steps/measures are put in place).

Assess

The General Manager, or assessing officer as determined by the General Manager in accordance with section 59G of the Act, will, within 30 days after the reporting Council officer first became aware of the suspected eligible data breach, carry out an assessment of whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach (an assessment).

Such assessment must be carried out in an expeditious way but is subject to an extension approved under section 59K of the Act.

During an assessment of a suspected eligible data breach, the General Manager will make all reasonable attempts to mitigate the harm done by the suspected breach.

Without limitation the assessor may consider the following when carrying out the assessment:

(i) the types of personal information involved in the breach,

(ii) the sensitivity of the personal information involved in the breach,

(iii) whether the personal information is or was protected by security measures,

(iv) the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given,

(v) the likelihood the persons specified in paragraph (iv)—

(a) have or had the intention of causing harm, or

(b) could or did circumvent security measures protecting the information,

(vi) the nature of the harm that has occurred or may occur,

(vii) other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

Notify

The General Manager must in the approved form, immediately notify the Privacy Commissioner of the eligible data breach.

Subject to an exception in the Act, as soon as practicable after the General Manager decides an eligible data breach occurred, the General Manager will, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify in accordance with section 59O:

(i) each individual to whom the personal information the subject of the breach relates, or

(ii) each affected individual.

If the individuals affected are not known or can't be identified, then Council will publicise the notification more broadly.

Council's media/communications department will be notified in order to prepare a media statement if appropriate in relation to the data breach.

Review

After the incident has been assessed and notification has taken place, Council's Public Officer should carry out a review within 14 days to identify any actions required to prevent further breaches to be tabled at a meeting of MANEX covering:

(i) Recommended changes to system and physical security;

(ii) Recommended changes to any Council policies or procedures;

(iii) Revision or changes recommended to staff training or education.

4.3 Eligible data breach incident register

The General Manager will establish and maintain an internal register for eligible data breaches. The register will include details of the following, where practicable, for all eligible data breaches:

(i) who was notified of the breach,

(ii) when the breach was notified,

(iii) the type of breach,

(iv) details of steps taken by the public sector agency to mitigate harm done by the breach,

(v) details of the actions taken to prevent future breaches, and

(vi) the estimated cost of the breach.

5. Delegations

Council's Public Officer is to review and make any necessary amendments to this Policy every 4 years or otherwise in accordance with any changes to the legislation.

6. Legislation

Privacy and Personal Information Protection Act 1998 (NSW)

Privacy and Personal Information Protection Regulation 2019 (NSW)

Local Government Act 1993 (NSW)

Local Government (General) Regulation 2021 (NSW)

Government Information (Public Access) Act 2009 (NSW)

7. Associated Council Documentation

Privacy Management Plan

Prviacy Statement

Model Code of Conduct

8. Version History

This section identifies authors who reviewed the Policy and the date that it became effective.

Version No.	Date changed	Modified by	Amendments/Previous adoption details