Data Breach Policy

	Name	Position	Signature	Date
Responsible Officer	Sue Mitchell	Manager Corporate & Community Services		11 December 2023
Authorised By	John Scarce	General Manager		11 December 2023

Document Revision History	
Date adopted by Council:	8 December 2023
Minute Number:	216/12/23
Revision Number:	
Review Date:	See item 6 of this Policy
Date adopted by Council:	
Minute Number:	
Next Review:	
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	

December 2023

Contents

1. Introduction

Amendments to the *Privacy and Personal Information Protection Act 1998* (PPIP Act) impact the responsibilities of agencies under the PPIP Act, and require agencies to provide notifications to affected individuals in the event of an eligible data breach of their personal or health information by a NSW public sector agency or state-owned corporation subject to the PPIP Act.

This policy provides guidance for responding to a breach of Murrumbidgee Council held data.

This policy sets out the Council procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists Murrumbidgee Council in avoiding or reducing possible harm to both the affected individuals/organisations and the Council, and may prevent future breaches.

The General Manager has overall responsibility for implementation of Murrumbidgee Council corporate policies.

2. Scope

This policy applies to all staff and contractors of Murrumbidgee Council. This includes temporary and casual staff, private contractors and consultants engaged by Council to perform the role of a public official.

This policy will apply from the date of adoption.

3. Purpose

The purpose of this policy is to provide guidance to staff in responding to a breach of Council held data, especially personal information.

This policy sets out the procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach and sets out the procedures for managing a data breach, including:

- providing examples of situations considered to constitute a data breach
- the steps involved in responding to a data breach
- the considerations around notifying persons whose privacy may be affected by the breach
- template correspondence for notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists Council in avoiding or reducing possible harm to both the affected individuals/organisations and the Council, and may prevent future breaches.

4. What is a data breach?

A data breach occurs when there is a failure that has caused, or has the potential to cause, unauthorised access to Murrumbidgee Council data, such as:

- accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, tablet or mobile phone, compact disk or USB stick)
- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted on to the Murrumbidgee Council website without consent
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to Murrumbidgee Council information or information systems
- equipment failure
- malware infection
- disruption to or denial of IT services

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

5. Responding to a data breach

The Murrumbidgee Council Public Officer, or General Manager nominee, must be informed of any data breach to ensure the application of this policy and advice to the General Manager/Information Commissioner to assist in responding to enquiries made by the public, and managing any complaints that may be received as a result of the breach.

The changes to the PPIP Act include:

- creating a Mandatory Notification of Data Breach (MNDB) Scheme which will require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
- applying the PPIP Act to all NSW state-owned corporations that are not regulated by the Commonwealth *Privacy Act 1988*
- repealing s117C of the *Fines Act 1996* to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

Agencies are required to comply with the mandatory notification provisions under Part 6A of the PPIP Act.

Under the MNDB Scheme, agencies have an obligation to:

- immediately make all reasonable efforts to contain a data breach
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach
- notify the Privacy Commissioner and affected individuals of the eligible data breach
- comply with other data management requirements.

There are four key steps required in responding to a data breach:

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat.

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Manager Corporate and Community Service and/or its service providers support Murrumbidgee Council in the supply and maintenance of its IT systems. The Manager or General Manager nominee will coordinate with the service providers to address and respond to identified data breaches related to its IT systems.

5.1 Step one: Contain a breach

All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that lead to the breach, revoke or change access codes or passwords.

If a third party is in possession of the data and declines to return it, it may be necessary for Murrumbidgee Council to seek legal or other advice on what action can be taken to recover the data. When recovering data, Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

5.2 Step two: Evaluate the associated risks

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

Some types of data are more likely to cause harm if compromised. For example personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list.

A combination of data will typically create a greater potential for harm than a single piece of data (for example an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- Who is affected by the breach? The Murrumbidgee Council assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- What was the cause of the breach? The Murrumbidgee Council assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?
- What is the foreseeable harm to the affected individuals/organisations? The Murrumbidgee Council assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information, personal information) subject to special restrictions under s.19(1) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) if it could be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage the Murrumbidgee Council's reputation?

5.3 Step 3: Consider notifying affected individuals/organisations

If, during assessment of the breach, it is decided that it is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach, affected individuals/organisations will be notified.

Murrumbidgee Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and is consistent with the Council's regulatory role. Notification demonstrates a commitment to open and transparent governance, consistent with the Council's approach.

Accordingly, Murrumbidgee Council adopts a relatively lower threshold in considering whether to notify individuals of the release or risk to the security of their personal information and will generally make such a notification. The Council will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the Council will consider when deciding whether notification is appropriate include:

- Are there any applicable legislative provisions or contractual obligations that require Council to notify affected individuals?
- What type of information is involved?
- What is the risk of harm to the individual/organisation?
- Is this a repeated and/or systemic issue?
- What risks are presented by the mode of the breach e.g. is it encrypted information or contained in a less secure platform e.g. email?
- Does the breach relate to casework functions and include case-related material flowing from the exercise of our regulatory functions?
- What steps has Council taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

Notification should be done promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. Considerations include the following.

5.3.1 When to notify

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

5.3.2 How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on Murrumbidgee Council's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm.

5.3.3 What to say

The notification advice will be tailored to the circumstances of the particular breach. Content of a notification could include:

- information about the breach, including when it happened
- a description of what data or personal information has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what Council is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what Council will do to assist people with this
- contact details for Council for questions or requests for information
- the right to lodge a privacy complaint with the Privacy Commissioner. The template at Appendix A will form the basis of this action.

5.4 Step four: Prevent a repeat

Murrumbidgee Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

5.5 Reporting Breach to General Manager

The template at Appendix B will be used for reporting on the investigation of the breach and authorising actions in response. The Public Officer will prepare a report using the template and provide to the General Manager who will review the proposed actions and recommendations of the report and approve.

The Public Officer will be responsible for the implementation of proposed actions and recommendations.

5.6 Notifying the Privacy Commissioner

If, during assessment of the breach, it is decided that it is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach, the NSW Privacy Commissioner will be notified of the breach where personal information has been disclosed and there are risks to the privacy of individuals. In doing so Council will ensure that relevant evidence is contained securely for access by the Privacy Commissioner should regulatory action be considered appropriate.

Such notification will:

- demonstrate to the affected individuals and broader public that Council views the protection of personal information as an important and serious matter and may therefore maintain public confidence in Council.
- facilitate full, timely and effective handling of any complaints made to the Privacy Commissioner in regard to the breach, and thus assist those whose privacy has been breached.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response Council has made to the breach
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person
- whether the breach has been notified to other external contact(s).

5.7 Recording of Data Breaches

An agency is required under section 59ZE to establish and maintain an internal register of eligible data breaches. This register should record the information specified under section 59ZE(2).

Agencies are required to maintain a public notification register of any notifications made under section 59N(2). The information recorded in the register must be publicly available for at least 12 months after the date of publication and include the information specified under section 59O.

6. Review

This Policy:

- To be reviewed within the first year of the new Council term;
- May be reviewed and amended at any time at Council's discretion (or if legislative or State Government policy changes occur).

Appendices

Appendix A

TEMPLATE CORRESPONDENCE

Dear [name]

I am writing to you with important information about a recent data breach involving your personal information / information about your organisation. The Information and Privacy Commission became aware of this breach on [date].

- A brief description of what happened.
- Description of the data that was inappropriately accessed, collected, used or disclosed.
- Risk(s) to the individual/organisation caused by the breach.
- Steps the individual/organisation should take to protect themselves from potential harm from the breach.
- A brief description of what Council is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.

Please call me with any questions or concerns you may have about the data breach.

We have established a section on our Council website [**insert link**] with updated information and links to resources that offer information about this data breach.

We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the [PPIP Act / HRIP Act / GIPA Act] you are entitled to register a complaint with the NSW Privacy Commissioner or NSW Information Commissioner/CEO with regard to this breach. Complaints may be forwarded to the following:

[insert Council details]

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me.

Yours faithfully,

Appendix B:

Template Report and Action

Description of data breach	Action Taken
When – What – How –	Notification – Containment –
Description of risks	**Action Proposed**
Risk – Harm – Affecting –	
Description of causes	**Action Proposed**
How – Why –	Change – Train – Remind – Review – Stop – Media – Remedy – Etc –
Notification to the NSW Privacy Commissioner	
Recommendations to Prevent Reoccurrence of Breach	

Public Officer or General Manager Nominee		Date:	
General Manager/ Information Commissioner Approved / Not Approved / Noted		Date:	