MANDATORY NOTIFICATION OF DATA BREACH POLICY

QUALITY CONTROL			
EDRMS REFERENCES	D23/50644		
RESPONSIBLE POSITION	Manager Information & Communications Technology		
APPROVED BY	Council		
REVIEW DATE	November 2025	**REVISION NUMBER**	1
EFFECTIVE DATE	**ACTION**	**MINUTE NUMBER**	
25 October 2023	Public Exhibition	47365	
20 December 2023	Adopted	47417	

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.

2. POLICY OBJECTIVE

The purpose of this policy is to provide guidance to employees in responding to a Data Breach of Broken Hill City Council held 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. It:

- Provides examples of situations considered to constitute a Data Breach;
- Details the steps to respond to a Data Breach; and
- Outlines the considerations around 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 Broken Hill City Council. It also provides the opportunity for lessons to be learned which may prevent future breaches.

3. POLICY SCOPE

This policy applies to all Broken Hill City Council employees.

4. POLICY STATEMENT

4.1 Council will form a Data Breach Review Team, whose role it is to investigate, respond and report internally on any known or notified Data Breach involving Confidential Information.

4.2 There are four key steps required in responding to a Data Breach. These are:

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

4.3 The first three steps may be undertaken concurrently.

4.3.1 Step 1: <u>Contain the breach</u>

4.3.1.1 Containing the Data Breach will be prioritised by Council. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover or request deletion of the information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

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

4.3.2 Step 2: <u>Evaluate the associated risks</u>

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

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

4.3.2.3 Given Council's regulatory responsibilities, release of case-related personal information will be treated very seriously. A combination of information 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).

4.3.2.4 Factors to consider include:

a) Who is affected by the Data Breach? Council will review 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.

b) What was the cause of the Data Breach? Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an 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 Confidential Information been recovered? Is the Confidential Information encrypted or otherwise not readily accessible?

c) What is the foreseeable harm to the affected individuals/organisations? Council's assessment will include reviewing what possible use there is for the Confidential Information. This involves considering the type of information (such as Health Information, Personal Information subject to special restrictions under s.19(1) of the Privacy and Personal Information Protection Act 1998 which 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 information? 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 Council's reputation?

4.3.3 Step 3: <u>Consider notifying affected individuals/organisations</u>

4.3.3.1 Council recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations.

4.3.3.2 Notification demonstrates a commitment to open and transparent governance, consistent with Council's values and approach.

4.3.3.3 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 counter productive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual, may cause unnecessary anxiety and desensitise individuals to a significant privacy breach.

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

a) Are there any applicable legislative provisions or contractual obligations that require Council to notify affected individuals?

b) What type of information is involved?

c) Who potentially had access and how widespread was the access?

d) What is the risk of harm to the individual/organisation?

e) Is this a repeated and/or systemic issue?

f) 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?

g) Does the breach relate to regulatory functions and include case-related material flowing from the exercise of our regulatory functions?

h) What steps has Council taken to date to avoid or remedy any actual or potential harm?

i) What is the ability of the individual/organisation to take further steps to avoid or remedy harm?

j) Even if Council would not be able to take steps to rectify the situation, is the information that has been compromised confidential, or likely to cause humiliation or embarrassment for the individual/organisation?

k) In situations when notification is required it should be done promptly to help avoid or lessen any potential damage by enabling the individual/organisation to take steps to protect themselves.

l) 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.

4.3.4 Considerations include the following:

When to notify

4.3.4.1 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 publicly reveal a system vulnerability.

How to notify

4.3.4.2 Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on 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.

What to say

4.3.4.3 The notification advice will be tailored to the circumstances of the particular breach.

4.3.4.4 Content of a notification could include:

a) information about the breach, including when it happened.

b) a description of what confidential or personal information has been disclosed.

c) what Council is doing to control or reduce the harm?

d) what steps the person/organisation can take to further protect themselves and what Council will do to assist people with this?

e) contact details for questions or requests for information.

f) the right to lodge a privacy complaint with the NSW Privacy Commissioner.

4.3.5 Step 4: Prevent a Repeat

4.3.5.1.1 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.

4.3.5.1.2 Preventative actions could include a:

a) Security audit of both physical and technical security controls

b) Review of policies and procedures

c) Review of staff/contractor training practices

d) Review of contractual obligations with contracted service providers.

4.3.6 Notifying the NSW Privacy Commissioner

4.3.6.1 As a matter of good practice, Council will notify the NSW Privacy Commissioner of a Data Breach where personal information has been disclosed and there are risks to the privacy of individuals.

4.3.6.2 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:

a) 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; and

b) 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.

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

a) A description of the breach

b) The type of personal information involved in the breach.

c) What response Council has made to the breach?

d) What assistance has been offered to affected individuals?

e) The name and contact details of the appropriate contact person.

f) Whether the breach has been notified to other external contacts.

4.3.7 Internal notifications

The following roles will be notified of any data breach:

- General Manager
- Director Corporate & Community
- Manager Information & Communications Technology
- Director Finance & Commercial
- Relevant Business Unit Manager
- Manager Corporate Risk

4.3.8 Data breach documentation

4.3.8.1 Documentation relating to data breaches will be stored in the Content Manager document management system.

4.3.8.2 An internal register of data breach incidents will be recorded in Vault.

4.3.8.3 An external register will be accessible on the Broken Hill City Council website for the public to access.

5. IMPLEMENTATION

The following Council officers are responsible for the implementation and the adherence to this policy.

5.1 Roles and Responsibilities

All employees will:

- Immediately report any actual or suspected Data Breaches to the Manager ICT.

The Manager Information & Communications Technology will:

- Immediately notify the Data Breach Review Team and assemble the Team as soon as possible.
- Undertake relevant internal notifications as required by this policy.
- Take immediate and any longer-term steps to contain and respond to security threats to Council's IT systems and infrastructure.

The Data Breach Review Team will:

- Assemble promptly to review and respond to a data breach.
- Follow this policy when responding to a data breach.

- Consult with internal and external stakeholders as required.
- Prepare a data breach review report for each separate Data Breach incident.

The Manager Corporate Risk will:

- Undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner
- Notify Council's insurers as required.

5.2 Communication

This Policy will be communicated to staff in accordance with Council's Policy, Procedure and Process Framework. Following approval by the General Manager, the Policy will be made available on Council's intranet.

6. ASSOCIATED DOCUMENTS

The following documentation is to be read in conjunction with this policy.

- Information and Privacy Commission (IPC) Data Breach Guidance for NSW Agencies
- NSW Mandatory Notification of Data Breach (MNDB) Scheme
- Information and Privacy Commission Data Breach Policy
- Information & Communications Technology Security Policy
- Privacy Management Plan

7. REVIEW

Review of this policy will incorporate relevant legislation, documentation released from relevant state agencies and best practice guidelines.

The standard review period will be within each term of Council following the Local Government Elections, or as required to ensure that it meets legislation requirements and the needs of the community and Council. The responsible Council officer will be notified of the review requirements three (3) months prior to the expiry of this policy.

The Manager Information & Communications Technology is responsible for the review of this policy.

8. LEGISLATIVE AND LEGAL FRAMEWORK

This policy is to be read in conjunction with the following:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*

Council employees shall refrain from personal activities that would conflict with proper execution and management of Council's Mandatory Notification of Data Breach Policy. Council's Code of Conduct provides guidance for recognising and disclosing any conflicts of interest.

9. DEFINITIONS

Term	Meaning
Broken Hill City Council Employee	Includes full time, part time, casual, temporary and fixed term employees, agency staff and contractors.
Confidential Information	Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, Security Classified Information and information related to the Broken Hill City Council IT/cyber security systems.
Council	Broken Hill City Council
Data Breach	For the purposes of this policy, a data breach occurs when there is a failure that has caused unauthorised access to, or disclosure of, Confidential Information held by Broken Hill City Council.
Data Breach Review Team	The core Data Breach Review Team comprises: • Manager Corporate Risk (or delegate) • Manager Information & Communications Technology • Manager Corporate & Customer Experience • Manager Communications & Marketing • Director Finance & Commercial Depending on the nature and circumstances of the breach, other employees may be called on to form part of the Data Breach Review Team.
IPC	Information and Privacy Commission
MNDB	NSW Mandatory Notification of Data Breach Scheme
PPIP ACT	*Privacy and Personal Information Protection Act 1998 (NSW)*