TEMORA SHIRE COUNCIL

DATA BREACH POLICY

ACTIVE

Review Details

ABOUT THIS RELEASE

DOCUMENT NAME: **Data Breach Policy**
CODE NUMBER: **G32**
AUTHOR: **Temora Shire Council**
ENDORSEMENT DATE: **May 2024**

REVIEW

Revision Date	Revision Description		Date approved by Council	General Managers Endorsement
April 2024	New Policy - Legislative Requirement	1	16 May 2024	MKB

PLANNED REVIEW

Planned Review Date	Revision Description	Review by
May 2028		

Contents

1. Policy Statement

Temora Shire Council is required under section 59ZD of the *Privacy and Personal Information Protection Act 1998* to prepare a Data Breach Policy and adhere to the NSW Mandatory Notification of Data Breach Scheme (MNDB).

The 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.

Council is committed to effective breach management, including notification where warranted, to assist in avoiding or reducing possible harm to both the affected individuals/organisations and Council. It also provides the opportunity for lessons to be learned which may prevent future breaches.

2. Scope

This policy applies to:

- Council staff
- Councillors
- Volunteers
- Contractors
- Subcontractors

3. References

- *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- *Health Records and Information Privacy Act 2002* (HRIP Act)
- Temora Shire Council Privacy Management Plan
- Notifiable Data Breaches 2018 (NDB) Scheme
- Mandatory Notification of Data Breach (MNDB) Scheme 2023

4. Implementation

While Councill is committed to protecting the privacy of personal and health information, there is always some risk of a data breach. In the event of an eligible data breach, Council will respond according to the process below, in accordance with the MNDB Scheme.

4.1 What is an eligible data breach?

An eligible data breach occurs where:

1. There is unauthorised access to or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency 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.

Some examples of data breaches include:

- accidental loss or theft of information or equipment on which information is stored (e.g., loss of a paper record, laptop, or USB stick)
- accidental or unauthorised disclosure of personal information (e.g., an email containing personal information is sent to the incorrect person)
- unauthorised access to information, or systems that hold information, by way of malicious behaviour, phishing attacks, or malware
- Publicly publishing a person's private information in a Council report, business paper or other communication

4.2 Responding to a data breach

If you believe there has been a data breach involving Council, you will need to notify the Privacy Officer, who will assist in assessing and managing the breach and work to make sure it does not happen again. All suspected or confirmed data breaches and 'near misses' must be reported immediately to the Privacy Officer.

To determine the nature of the breach, Council will consider:

- the type of information that was disclosed
- the number of individuals affected, and
- the risk of harm that could be caused to individuals and Council by the breach.

Council will take the following steps to manage a data breach.

Contain
Council will take immediate actions to contain the breach to minimise any resulting damage or harm.

Evaluate
Council will undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach.

During this assessment period, Council will make all reasonable attempts to mitigate the harm done by the suspected breach.

During any assessment, Council will decide whether a breach is an eligible data breach or there are reasonable grounds to believe the data breach is an eligible data breach.

To determine the following steps, the type of information involved in the breach will be assessed, including any risks associated with the breach. This will also include assessing what caused the breach, who has been impacted, and any foreseeable harm to the affected individuals/organisations.

Notify
In accordance with the MNDB Scheme being introduced, and other changes to the PPIP Act effective from 28 November 2023, Council will provide notifications to the Privacy Commissioner and affected individuals in the event of an eligible data breach of an individual's personal or health information.

Council will notify the individuals/organisations affected as soon as possible to enable them to take any steps needed to protect themselves and advise them of their rights to complain to the Privacy Commissioner.

Council may decide not to notify in some circumstances if notification is likely to cause more harm than it would alleviate.

Council's default position is to voluntarily report data breaches to the Privacy Commissioner. Refer to the NSW IPC website for more on data breach notification.

Council may be required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific remediation or containment steps or engaging with or notifying external stakeholders in addition to the Privacy Commissioner, where a data breach occurs.

Act
Any additional action identified to mitigate risks or harm will be implemented.

Prevent
Council will identify steps it can take to prevent similar breaches from occurring.

4.3 Data breach Incident register

Council will maintain an internal register for eligible data breaches. Each eligible data breach will be entered on the register and will include where practicable:

- Who was notified
- When the breach was notified
- The type of breach
- The details of steps taken by Council to mitigate harm done by the breach
- The details of the actions taken to prevent future breaches
- The estimated cost of the breach

4.4 Data breach notification register

Council will maintain and publish a notification website on its website. This register will include any public data breach notification issued by Council.

A public data breach notification is a notification made to the public at large rather than a direct notification to an identified individual.

The data breach notification register will include public data breach notifications.

4.5 Public data breach notification

The MNDB Scheme provides for a public data breach notification to occur in two circumstances:

1) Council **must** make a public notification if it is unable, or it is unreasonably practicable to notify any or all of the individuals affected by the data breach directly, or

2) Where the General Manager decides to make a public notification. The issuing of a public notification under these circumstances does not excuse Council from the requirement to make direct notifications to affected individuals if it is reasonably practicable to do so.

The PPPIP Act does not prescribe the information that must be included in the register. However, the purpose of the register is to ensure that individuals are able to access sufficient information about a data breach to determine whether they may be affected by the breach and take action to protect their personal information.

Council will provide the following information on the public data breach notification register:

- What happened
- What has been accessed
- What the agency is doing, and
- What an affected individual can do

5. Appeal/objections process

5.1 Making a privacy complaint

To enquire how Council handles your personal information or raise a concern, please contact Council's Privacy Officer. The Privacy Officer can be reached at:

Temora Shire Council
Phone: 02 6980 1100
Email: temshire@temora.nsw.gov.au
Mail: PO Box 262 Temora NSW 2666

Council encourages informal resolution of privacy issues. However, if you believe Council has breached the PPIP Act or HRIP Act about your personal information, you have the right to seek a formal process known as an 'internal review'.

5.2 Internal Review

An internal review under Part 5 of the PPIP Act is an internal investigation that the Council conducts into a privacy complaint. Council will assess the complaint and if it has complied with the privacy principles and then communicate the findings with the applicant.

Applications for an internal review must:

- be in writing (we recommend using the internal review application form developed by the NSW Information & Privacy Commission)
- be addressed to Council's Privacy Officer
- be made within six months of when you first became aware of the conduct, and
- be related to your personal information (including health information).

Upon receiving the application, the Privacy Officer will appoint a Reviewing Officer to conduct the internal review. The Reviewing Officer must not be substantially involved in any matter relating to the application and must be suitability qualified.

Council will complete the internal review as reasonably practicable in the circumstances. If the review is not completed within 60 days, you can seek an 'external review'.

The Council must notify the Privacy Commissioner of an internal review application as soon as practicable after its receipt, keep the Commissioner informed of the progress of the review, and notify the Commissioner of the findings and the action it proposes to take. Council may also provide a copy of any submission by the Privacy Commissioner to the applicant.

Council will notify the applicant in writing within 14 days of completing the internal review of:

- the findings of the review
- actions proposed to be taken by Council (if any), and
- the right of the applicant to have their complaint reviewed by the NSW Civil and Administrative Tribunal ('external review').

A copy of the final review report should also be provided to the Privacy Commissioner, where it departs from the draft review report.

An internal review checklist has been prepared by the NSW Information & Privacy Commission and can be accessed from its website http://www.ipc.nsw.gov.au

5.3 Role of the Privacy Commissioner

The Privacy Commissioner has an oversight role in how agencies handle privacy complaints and is entitled to make submissions to Council about internal reviews. Council is required to consider any relevant material submitted by the Privacy Commissioner. Council must provide the Privacy Commissioner with a draft of Council's internal review report to enable the Privacy Commissioner to make a submission.

5.4 External review

If the applicant disagrees with the outcome of an internal review or is not notified of an outcome within 60 days, they have a right to seek an external review. The applicant can appeal a decision to review Council's conduct to the NSW Civil and Administrative Tribunal (NCAT). An appeal must be lodged with NCAT within 28 days of Council's determination. NCAT may order Council to change its practices, apologise or take steps to remedy any damage. NCAT may also award compensation if warranted.

Contact details for NCAT are:

NSW Civil and Administrative Tribunal
Administrative and Equal Opportunity Division
Phone: 1300 006 228
Level 10, John Maddison Tower,
86-90 Goulburn Street,
HAYMARKET NSW 1240
Mail: PO Box K1026, SYDNEY NSW 2000

Alternative to Lodging an Internal Review

If a person does not want to apply for internal review with Council, they may contact the Privacy Commissioner directly, not as an external review mechanism, but as a complaint.
The contact details for the Privacy Commissioner are:
NSW Information and Privacy Commission

Phone: 1800 472 697
Email: ipcinfo@ipc.nsw.gov.au
Mail: PO Box 7011, SYDNEY NSW 2001

5.5 Related Policies

Privacy Management Plan
Data Breach Procedure
Code of Conduct
Records & Information Management Policy
Risk Management Policy