NSW Mandatory Notification of Data Breach Scheme - Data Breach Policy

1. PURPOSE

This policy outlines Tamworth Regional Councils (Council) approach to a data breach that is constituted under the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act), and which is notifiable to the Privacy Commissioner under the NSW Mandatory Notification of Data Breach Scheme (MNDB). It provides guidance to Council staff and the community on how to prepare for and restrict harm to an individual as a result of a data breach, and also describes Council's procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

This policy does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Tamworth Regional Council will continue to respond to other types of data breaches in accordance with relevant policies and procedures.

2. COMMENCEMENT OF POLICY

This Policy commences on 28 November 2023 and will be reviewed at least annually.

3. APPLICATION OF THE POLICY

Council is committed to protecting all data held about an individual, but now has explicit obligations, and is bound by the MNDB scheme.

3.1. Council Obligations

Council general obligations:

- Making this Data Breach Policy publicly available
- Maintaining an internal Eligible Data Breach Incident Register, and
- Maintaining a Public Notifications Register on the Council website that provides a summary of eligible data breaches where certain circumstances are met.

Council specific obligations should a data breach be identified:

- Immediately make all reasonable efforts to contain the breach
- Undertake an assessment within 30 days where there are reasonable grounds to suspect an eligible data breach has occurred
- During the assessment period make all reasonable attempts to mitigate harm done by the suspected breach
- Decide whether a breach is an eligible data breach or that 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

3.2. Data covered by this policy

The MNDB scheme applies to:

- 'Personal information' as defined in section 4 of the PIPP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, and
- 'Health information' as defined in section 6 of the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act), meaning information about an individual's physical or mental health, disability, and personal information connected to the provision of a health service.

3.3. Elements of a data breach

An 'eligible data breach' occurs where:

- There is an unauthorised access to, or unauthorised disclosure of, personal information held by Council 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
- A reasonable person would conclude that the access to or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

For the purposes of this policy, 'serious harm' can include physical, financial, material, emotional, psychological or reputational harm. This policy however recognises that the impact of the harm can vary from person to person and this will be taken into consideration when assessing whether a data breach is an eligible data breach.

Importantly, an eligible data breach may be accidental or deliberate and may occur across a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive information or systems, inadvertent disclosure, social engineering or hacking.

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
- The browsing of personal information or health information held by Council without a legitimate purpose
- Publicly publishing a person's private information in a Council report, business paper or other communication

3.4. Exemptions from the obligations of the MNDB scheme

There is only one exemption available to Council from temporarily meeting its obligations under the MNDB scheme:

- Where the General Manager reasonably believes that notification of an eligible data breach would worsen Council's cyber security or lead to further data breaches, the General Manager may decide to exempt Council, for a temporary period of time, from its requirement to notify affected individuals or make a public notification.

Should this exemption be applied, Council will notify the Privacy Commissioner by written notice of the exemption period and methods being undertaken to review the exemption period, e.g., Council will review the exemption each month should the exemption period extend beyond one month.

For the purposes of applying this exemption:

- 'Reasonable belief' is a belief that results from the exercise of sound judgement and which is based on the information available
- 'Cyber security' are the measures used to protect the confidentiality, integrity, and availability of systems and information.

4. COUNCILS APPROACH TO MANAGING A DATA BREACH

In preparing to meet its obligations under the PPIP Act and MNDB scheme, Council has established a Privacy MNDB Response Team (Response Team), with members from key business units, who will manage Council's responsibilities under this policy and in accordance with Councils Data Breach Response Plan.

In addition, Council:

- Maintains an effective and integrated risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation;
- Has a range of supporting policies to control and mitigate exposures to breaches of data; and
- A comprehensive set of information technology controls which includes robust access controls, data encryption, network and endpoint security measures, data loss prevention systems, and incident response plans.

4.1 Data Breach response Steps

When identifying or being notified of a possible or confirmed data breach, the Response Team will follow five key steps:

1. **Triage** and perform an initial assessment of the suspected data breach as soon as practicable to determine whether there are reasonable grounds to suspect an eligible data breach with consideration to the type of information that was disclosed, the number of individuals affected, and the potential risk of harm that could be caused to individuals and Council by the breach.
2. **Contain** the data breach to minimise possible damage or harm.

3. **Assess** within 30 days of identifying or being notified, the information involved in the breach and the risks associated to determine whether an eligible data breach has occurred, next steps required, and any additional actions needed to further mitigate risks, damage, or harm. In the event of an eligible date breach being confirmed, details of this will be added to the internal Eligible Data Breach Incident Register.
4. **Notify** affected individuals and the Privacy Commissioner if assessed as an eligible data breach. Public notification will also be made with details of the eligible data breach being added to the Public Notifications Register on Council's website.
5. **Prevent** a repeat of the data breach by conducting a post incident review and implementing necessary preventative actions identified.

4.2 Notifying a Data Breach to Council

If you believe there has been a data breach involving Council, you can notify this to the Response Team by email to: privacymndb@tamworth.nsw.gov.au, or in writing to:
PO Box 555,
Tamworth, NSW 2340.

All suspected or confirmed data breaches identified by Council staff, including contractors or third parties engaged by Council, **MUST** be reported immediately to the Response Team.

4.3 Council notifying you if you're affected by an Eligible Data Breach

If Council determines that you are affected by an eligible data breach, Council will make all reasonable efforts to notify you in writing and advise:

- The date the breach occurred, a brief description of what happened, and the type of breach that has occurred
- A description of the personal information or health information that is the subject of the eligible data breach
- The actions taken by Council or planned to be taken by Council to take to control or mitigate the harm done to you
- The steps you should consider taking yourself
- Information about how to seek an internal review of the agency's conduct or how to make a privacy complaint to the Privacy Commissioner.

Council may, depending on the circumstances of the eligible data breach, provide assistance to replace compromised government issued identity documents or credentials such as a driver's licence.

4.4 Internal Eligible 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:

- Those notified of the breach
- When the breach was notified
- The type of breach
- Details of the steps taken by Council to mitigate harm done by the breach

- Details of the actions taken to prevent future breaches
- The estimated cost of the breach

4.5 Public Notifications Register

Council will maintain its public notifications register of eligible data breaches on Council's website, where it will publish notifications in circumstances where notification to individual affected persons by an eligible data breach cannot be achieved or where notification to any or all impacted individuals is not reasonably practicable. The General Manager may also, under some circumstances, make a public notification on the public notification register even if impacted individuals have been notified.

A public notification will remain on the public notifications register for at least 12 months from the date of notification was first published.

4.6 Notifications to the Privacy Commissioner

Mandatory notifications to the Privacy Commissioner of an eligible data breach will be made using the form provided by the Information and Privacy Commission.

POLICY VERSION AND REVISION INFORMATION

Policy Authorised by: Paul Bennett	Next Scheduled Review: November 2024
Title: General Manager	Current version: 01