Narrandera
Shire Council

Data Breach Policy 2024

POL164

Policy No:	**POL164**
Policy Title:	**Data Breach Policy**
Section Responsible:	**Information Technology**
Minute No/Ref:	**5.6 710844**
Doc ID:	**706479**

1. INTENT

The Data Breach Policy outlines Narrandera Shire Council's (NSC) methodology to complying with the NSW Mandatory Notification of Data Breach (MNDB) Scheme, the roles and responsibilities for reporting data breaches and managing a data breach so that the breach is contained, assessed, and responded to, as quickly as possible.

2. SCOPE

This policy is applicable and must be complied with by:

- All NSC permanent full time, part time, trainee and temporary staff, councillors, volunteers, contractors, consultants, and vendors engaged by NSC.
- Anyone authorised to access and make use of any NSC computing systems, networks and/or information; and
- Any other body authorised to administer, develop, manage and support NSC Information systems and assets.

3. OBJECTIVE

The objective of the Data Breach Policy is to establish Council's approach to identify and manage a Data Breach, including:

- Definition of a data breach including common examples.
- The Data Breach Response Plan.
- The five steps of data breach management.
- Assist NSC to meet its legal obligations in respect of Mandatory Reporting Data Breaches under the Privacy and Personal Information Protection Act 1998.

4. POLICY STATEMENT

The *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) Part 6A determines the NSW Mandatory Notification of Data Breach (MNDB) Scheme. The scheme expects every NSW public sector agency required by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches. Public sector agencies are required to prepare and publish a Data Breach Policy to manage eligible breaches plus maintaining an internal register and public register of eligible data breaches.

NSC is committed to ensuring the confidentiality, integrity and availability of its clients' information and the information of the whole organisation.

5. PROVISIONS

5.1 DATA BREACH DEFINITION

An eligible data breach under the MNDB scheme occurs when the following two tests are satisfied:

1. Personal information held by NSC (either digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in situations where the loss is 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.

Serious harm is not defined in the PPIP Act but could include examples such as physical harm; economic, financial, or material harm; emotional or psychological harm and reputational harm where the consequence arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The impact on the individual must be more than simple irritation, annoyance, or inconvenience.

Data breaches can be caused by human error, systems failure or malicious activities with common examples including:

- Accidental loss or theft of information assets on which unencrypted data is stored such as loss of paper record or upload of data to unsecure file sharing platform.
- A letter or email is sent to the wrong recipient.
- A physical asset such as a paper record, laptop, tablet, USB stick or mobile phone containing personal identifiable information is lost.
- Unauthorised sharing of information with other internal staff or external entities.
- Malware or ransomware infection.
- IT systems not maintained through the application of known and supported patches.
- Social engineering or impersonation leading into inappropriate disclosure of personal information.

5.2 DATA BREACH RESPONSE PLAN

NSC has developed a Data Breach Response Plan to respond efficiently to a data breach. The plan details the roles and responsibilities for handling an appropriate response to a data breach as well as describing the actions to be taken by NSC in managing a breach if one is identified. The Data Breach Response Plan is managed by the IT section.

Where a suspected data breach is identified, staff or the third-party personnel should notify the relevant Manager or Deputy General Manager within one day advising of the suspected data breach and the Data Breach Response Plan should be initiated.

Suspected eligible data breaches are to be reported directly to the General Manager. NSC has 30 days to assess if an incident is an eligible data breach and who needs to be notified.

5.3 DATA BREACH MANAGEMENT

The five key steps in the process of responding to a Data Breach include:

1. Report and triage
2. Contain the breach.
3. Assess and mitigate
4. Notify relevant authorities and affected individuals
5. Review.

Steps 1 - 3 will be required for all Data Breaches.

Steps 4 and 5 only need to be followed if the breach results in any notification or review requirements. Each step will be considered, and appropriate actions taken through the Data Breach Response Plan depending on the nature, severity, and impact.

5.4 NON-COMPLIANCE

The IT section is to be informed immediately of any actual or suspected breach of this policy. Non-compliance or breaches of this policy, without an appropriate exception, will be investigated and misconduct escalated, which may result in disciplinary action in accordance with NSC policy.

5.5 CONTACT WITH AUTHORITIES

Every contact involving authorities about an eligible data breach will be initiated by the General Manager or their delegate within the required timeframes.

6. DEFINITIONS

- See Appendix 1

7. ROLES AND RESPONSIBILITIES

7.1 EXECUTIVE LEADERSHIP TEAM

- ELT is responsible for enforcing the principles of the Data Breach Policy.

7.2 IT TEAM

- The IT team has responsibility for monitoring compliance and reviewing and updating this policy when any significant new information, legislative or organisational change warrants amendments to this document.
- Providing advice and support about this policy.

7.3 ANYONE AUTHORISED TO ACCESS AND MAKE USE OF ANY NSC COMPUTING SYSTEMS, NETWORKS AND/OR INFORMATION

- All staff, councillors, volunteers, contractors, consultants, vendors have a duty to immediately report suspected data breaches to their Manager, a Deputy General Manager or the General Manager.
- Information security is an issue that affects all staff and associated persons at NSC. All of these persons must use common sense and take an active role in security. See Appendix 2 – Engaging Information Security for assistance identifying when to engage information security.

8. RELATED LEGISLATION

- Health Records and Information Privacy Act 2002
- Local Government Act 1993
- Privacy Act (Cth) 1988
- Privacy Amendment (Enhancing Privacy Protection) Act (NSW) 2012
- Privacy and Personal Information Protection Act 1998
- Public Finance and Audit Act 1983.

9. RELATED POLICIES AND DOCUMENTS

- Cyber Incident Response Plan
- POL149 Information Security Policy
- POL150 Data Privacy and Protection Policy
- POL151 Access Control Policy
- POL152 IT Security Policy
- POL153 IT Acceptable Use Policy
- POL154 Cloud Security Policy

10. VARIATION

Council reserves the right to review, vary or revoke this policy in accordance with legislation, regulation, and award changes, where applicable. Council may also make charges to this policy and the relevant procedures from time-to-time to improve the effectiveness of its operation.

11. PREVIOUS VERSIONS

Reference to a superseded policy number and/or name is also considered a reference to the new policy number. This policy was previously named:

- Not Applicable.

POLICY HISTORY

Responsible Officer	**Information Technology Manager**		
Approved by	**General Manager**		
Approval Date	**14 March 2024**		
GM Signature	George Cowan		
Next Review	**1 June 2026**		
Version Number	**Endorsed by ELT**	**Endorsed by Consultative Committee and/or WHS Committee**	**Date signed by GM**

1 Adopted	25/01/2024	-	14/03/2024
2 Reviewed	DD/MM/YYYY	-	DD/MM/YYYY
2 Reviewed	DD/MM/YYYY	-	DD/MM/YYYY

NOTE: This is a controlled document. If you are reading a printed copy, please check that you have the latest version via Council's website (external) or MagiQ (internal). Printed or downloaded versions of this document are uncontrolled.

12. Acknowledgement of Training Received

I hereby acknowledge that I have received, read and understood a copy of Council’s Data Breach Policy.	
Employee Name	
Position Title	
Signature	
Date	

Appendix 1: Definitions Abbreviations Acronyms

Term	Definition
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Outsourcing	Outsourcing includes any commercial arrangement where an external party stores, transfers, uses or creates NSC information and data. This is however separate from an information sharing venture.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course.

Term	Abbreviation/Acronyms
ELT	Executive Leadership Team
IT	Information Technology
MNDB	Mandatory Notification of Data Breach
NSC	Narrandera Shire Council
PPIP	Privacy and Personal Information Protection

Appendix 2: Engaging Information Security

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, contact the IT Team immediately.

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of NSC information, services or assets?
- Are you procuring a service from a third party which sees NSC information being stored, used, created or processed by the third party?
- Are you sharing NSC information with an external party?

If you answer yes to any of the above, email the IT Team ASAP