# DATA BREACH POLICY

| | |
|---|---|
| **Responsible Department:** | Financial and Commercial Services |
| **Responsible Section:** | Customer and Information Services |
| **Responsible Officer:** | Manager Customer and Information Services |

## Objective

The purpose of this policy is to provide guidance to Council employees in responding to a Data Breach of 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 the Council in avoiding or reducing possible harm to both the affected individuals/organisations and the Council. It also provides the opportunity for lessons to be learned which may prevent future breaches.

## Introduction

Data is an important business asset that must be protected. Council holds data in accordance with the Information Protection Principles, the Health Privacy Principles, and applicable laws and contractual obligations.

Robust data breach management will assist Council in complying with its statutory duty to protect data. This policy aims to ensure that:

- Data breaches are reported as soon as they are identified;
- Data breaches are assessed and managed systematically;
- Affected individuals and entities are notified of a data breach; and
- Data breaches are accurately recorded.

## Policy

### 1. Definitions

| Term | Meaning |
|---|---|
| **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 Council's IT/cyber security systems. |
| **Council Employee** | Includes full time, part time, casual, temporary and fixed term employees, agency staff and contractors. For the purposes of this policy, employees also include volunteers, trainees and students on work placements. |



Document Set ID: 2117870
Version: 1, Version Date: 30/11/2023

| | |
|---|---|
| **Data Breach** | The loss, unauthorised access, modification, disclosure, misuse, or interference with information held by Council, whether personal information, health information, or other information. |
| **Data Breach Review Team** | Manager Governance and Risk<br>Manager Customer and Information Services<br>Director Financial and Commercial Services<br>Senior Corporate Risk Advisor<br>Or their delegates<br><br>Depending on the nature and circumstances of the breach, other employees may be called on to form part of the data breach review team. |
| **Eligible Data Breach** | A Data Breach of Health and/or Personal Information where a reasonable person would conclude that the breach would be likely to result in serious harm to an individual to whom the information relates. |
| **Health Information** | A specific type of Personal Information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results. |
| **Personal Information** | Information or an opinion (including information or an opinion forming part of a database and whether or not in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. This includes, for example, their name, address, email address, phone number, date of birth or photographs. |
| **Privacy Commissioner** | The Privacy Commissioner appointed under the provisions of the Privacy and Personal Information Protection Act. |
| **Unauthorised Access** | Any access of Council's records, data, and information that is not duly authorised and/or is not for lawful and legitimate Council purposes. |

# Part 1: Application

## 2. Application

3. This policy is a joint policy of the Council and General Manager. To the extent that this policy directs staff in their duties, that direction is made on the authority of the General Manager. Such Directions do not take effect until the General Manager has signed this policy or otherwise unambiguously confirmed in writing that the directions have commenced.
4. The General Manager may not alter directions contained in this policy without the endorsement of Council.

# Part 2: Overview

## 5. Overview of Procedure

6. Narrabri Shire Council follows the below procedure in responding to data breaches:


7. Each step is described in detail below. Some steps may occur simultaneously depending on the circumstances of each case.

## Part 3: Identification

### 8. Staff Responsibilities

9. If a staff member identifies or suspects a data breach, they must immediately lodge an IT ticket by email. The ticket should, at a minimum, contain the following information:
    (a) What information they know or suspect has been subject to a data breach;
    (b) When they know or suspect the data breach to have occurred;
    (c) The nature of the data breach; and
    (d) Any people they know or suspect to be involved in the data breach.
10. The email should cc Manager Governance and Risk (or If Manager Governance and Risk is suspected to be involved in the breach, the General Manager).

### 11. Information Services Responsibilities

(a) Upon receipt of an IT Ticket reporting a real or potential data breach, Information Services must immediately notify all members of the Data Breach Review Team via email.

## Part 4: Triage

### 12. First Steps

13. The Data Breach Review Team will meet within 2 hours of referral, or as soon as practicable. The meeting can be in person, via a teleconference, or a combination of the two (provided teleconference software is not compromised).
14. At this meeting, the team will:

(a) Assign a member of the Team as Lead Investigator, to assess and manage the data breach in accordance with this Policy;
(b) Notify MANEX if the breach is determined to potentially amount to a major breach; and
(c) Appoint somebody to provide support and guidance to the staff member that identified the breach.

### 15. Privacy/Health Data Breaches

16. If the suspected or confirmed data breach involves, or may involve, personal or health information, the team must appoint Manager Governance and Risk as the Lead Investigator.
17. The General Manager delegates their functions under section 59ZJ of the *Privacy and Personal Information Protection Act 1998* (NSW), as head of the organisation for the purpose of Part 6A of that Act, to Manager Governance and Risk.
18. If Manager Governance and Risk is unable to fulfil these functions, or if they are suspected or known to have involved in the data breach, then the General Manager will delegate this authority as they see fit, and the Committee will appoint an alternate Lead Investigator.
19. If the Lead Investigator is satisfied that an assessment cannot reasonably be conducted within 30 days of the data breach, they may approve an extension of the period to assess the breach. The extension may be for a period of time the Lead Investigator determines to be reasonably required for the assessment to be conducted.
20. If an extension is approved under 7.4 above, the Lead Investigator will, within 30 days of the breach, commence the assessment and give written notice to the Privacy Commissioner that assessment has commenced, and an extension has been approved.
21. If the assessment is not concluded by the extended date for completion, the Lead Investigator must give written notice to the Privacy Commissioner of the new extension period.

## Part 5: Contain and Assess

### 22. Containment

23. The Lead Investigator will contain the breach and conduct a preliminary assessment.
24. The breach will be contained by immediately making all reasonable efforts to:
    (a) Stop the unauthorised activity;
    (b) Recover or limit the dissemination of records disclosed without authorisation; and/or
    (c) Shut down any compromised systems.

### 25. Assessment

26. The Lead Investigator will undertake an assessment to determine:
    (a) The information involved in the breach;
    (b) If the breach involves personal and/or health information, the type of personal and/or health information the breach involves;
    (c) Whether the breach involves a loss of personal and/or health information;
    (d) Whether it is likely that the breach will result in unauthorised access to, or disclosure of, the information;
    (e) Whether a reasonable person would conclude that the breach will likely result in serious harm to an individual to whom the information relates;
    (f) The number of people affected, or likely to be affected, by the breach;
    (g) How the information could be used;
27. In determining 9.1(e) above, the Lead Investigator will have reference to:
    (a) The type of information involved;

(b) The sensitivity of the information involved;
(c) Whether the information is or was protected by security measures (such as encryption or password protection) and is therefore unlikely to be accessed or misused;
(d) Who had access to the information;
(e) Whether the person who accessed the information may have had malicious intent and whether they were capable of circumventing security measures; and
(f) The general nature of harm that has or may occur.

# Part 6: Notification

## 28. Notifying the Privacy Commissioner

29. If the Lead Investigator has reasonable grounds to suspect or conclude that an eligible data breach has occurred, they must immediately notify the Privacy Commissioner in accordance with the Act and this Policy, or as soon as reasonably practicable.

## 30. Notifying Affected Individuals

31. If the Lead Investigator has reasonable grounds to suspect or conclude that an eligible data breach has occurred, they must notify each individual to whom the health or personal information to which the breach relates, or their authorised representative, in writing about the breach as soon as reasonably practicable, unless exempt from doing so.
32. The notification to affected individuals must contain an accurate description of what happened, what risks may arise, and what they can do to protect themselves. The notification must, at a minimum, contain the following:
    (a) The date of the breach;
    (b) A description of the breach;
    (c) An explanation of how the breach occurred;
    (d) The type of breach that occurred;
    (e) The health or personal information that was subject of the breach;
    (f) The amount of time the information was disclosed for, accessible, or otherwise outside the control of Council;
    (g) Actions Council has taken to ensure the information is secure;
    (h) Actions Council has taken to control or mitigate the harm caused to the individual;
    (i) Recommendations about what the individual should consider doing in response to the eligible data breach; and
    (j) Information about:
        (i) How to make a privacy related complaint to the IPC;
        (ii) How to make an internal complaint about Council's conduct;
        (iii) The contact details of a person in Council nominated to be a contact for the affected individual or entity.

33. If it is not reasonably practicable to directly notify any or all affected individuals, the Lead Investigator will:
    (a) Arrange for a public notification to be published on Council's website for at least twelve months containing the elements in 11.2 above except (e).
    (b) Ensure that the public notification remains on Council's website for at least 12 months;
    (c) Take reasonable steps to publicise the notification; and
    (d) Provide the Privacy Commissioner with information about how to access the public notification.

## 34. Notifying Other Entities

35. In consultation with the Team and relevant officers of Council, the Lead Investigator will determine if it is appropriate and necessary to notify third parties, such as:
    (a) Police
    (b) Insurance Providers;
    (c) Financial Institutions;
    (d) Professional/regulatory bodies;
    (e) Other internal or external parties that have not yet been notified;
    (f) Agencies that have a direct relationship with the information that is subject of the breach.

### 36. Notifying the Reporting Staff Member

37. The person appointed by the Data Breach Review Team will notify the reporting staff member of the outcome of the data breach and assist them in responding to any requests for information relating to the breach from stakeholders or other third parties.

## Part 7: Risk Assessment

### 38. Assessing the Risk

39. The Lead Investigator will conduct a risk assessment around the following areas:
    (a) The cause of the breach;
    (b) The extent of the breach;
    (c) The likelihood of ongoing or repeated breaches;
    (d) Evidence of theft;
    (e) Whether there is a systemic problem in Council;
    (f) Other harm potentially caused by the breach;
    (g) Whether there have been other breaches that amount to a cumulative breach;
    (h) Whether the information has been recovered/is recoverable;
    (i) The controls already taken to mitigate harm;
    (j) Reputational risk to Council
    (k) Other risks to Council
40. Each risk arising from the risk assessment must be entered into Council's Risk Management System for treatment under the Risk Management Framework. They must be flagged with an appropriate flag so as to identify and categorise all risks associated with the breach.
41. Access to risks entered into Council's Risk Management System should be restricted so far as is reasonably practicable.

## Part 8: Review and Prevention

### 42. Review by Lead Investigator

43. Once immediate steps have been taken as above, the Lead Investigator will ensure that the breach is fully investigated to identify the root causal and contributing factors to the breach.
44. The Lead Investigator will provide a report to the Data Breach Review Team following this investigation.

### 45. Review by Data Breach Review Team

46. The Lead Investigator must make a report to the Data Breach Review Team as soon as reasonably practicable following completion of each of the Risk Assessment step, or at any other time the Lead Investigator deems appropriate.

47. The Lead Investigator must report its investigation findings to the Team within 14 days of completion of the investigation.
48. The reports should contain sufficient information to inform the Team in its duties.

## 49. Review by the Management Executive Committee

50. At intervals the Team deems necessary, or at least following receipt of the investigation report, the Team should submit a report to MANEX outlining:
    (a) The nature of the breach;
    (b) Steps taken to respond to the breach;
    (c) Notifications made: and
    (d) Future steps required to respond to the breach.
51. MANEX will, in consultation with the Data Breach Review Team, and other relevant experts, ensure that a plan is prepared to mitigate the risks identified in the Risk Assessment. Such a plan will include:
    (a) The risks to be addressed;
    (b) A desired "end-state" containing outcomes sought;
    (c) Controls consisting of measurable actions to address those risks;
    (d) The person responsible and accountable for the overall plan's completion;
    (e) The person responsible for each action/outcome;
    (f) A review mechanism to allow Council to be satisfied that it has reached its desired end-state.

## 52. Review by ARIC

53. A report will be brought to each ARIC meeting during the process of responding to any breach, and until all controls arising from the risk assessment and prevention measures have been completed.
54. The report shall contain sufficient information to enable ARIC to fulfil its functions.

## 55. Review of Policy

56. This policy will be reviewed within 12 months of an Ordinary Council Election or other such time on an as-needs basis.

# References

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *State Records Act 1998* (NSW)

# History

| Minute Number | Date | Description of Change |
|---|---|---|
| 311/2023 | 28 November 2023 | Adopted |