# DATA BREACH NOTIFICATION POLICY

## March 2024

**PREPARED BY:**

**INFORMATION MANAGEMENT & TECHNOLOGY UNIT**

4-20 Eton Street,
Sutherland NSW 2232
T 02 9710 0333
**sutherlandshire.nsw.gov.au**

# DATA BREACH NOTIFICATION POLICY

## 1. PURPOSE

Council holds and is trusted with personal, health, confidential and sensitive data relating to its people, customers and the community. Data breaches can have significant consequences for individuals, organisations and agencies. This Policy outlines Council's principles and commitment in responding to an eligible data breach as required by the Mandatory Notification of Data Breach Scheme.

## 2. COMPLIANCE

Council is required to the report eligible data breaches under the *Privacy and Personal Information Protection Act 1998* (NSW).

An eligible breach occurs when there is unauthorised access or disclosure of information that a reasonable person would conclude would likely result in serious harm to an individual (to whom the information relates).

## 3. APPLICATION

This Policy applies to all Council employees, Councillors and contractors and volunteers of Sutherland Shire Council who provide or handle Council data.

## 4. PRINCIPLES

### 4.1 Application of Principles

No one principle should be applied to the detriment of another. Principles must be collectively considered and applied to the extent that is reasonable and practicable in the circumstances.

### 4.2 Openness and Transparency

Council is committed to the principle of an open and transparent government. Council will meet the obligations of the Mandatory Notification of Data Breach Scheme by:

- Publishing a public register of data breach notifications on Council's website.
- Maintaining an internal register of eligible data breaches.

### 4.3 Commitment to Security and Protection of Personal Information

Council will follow its obligations to maintain the Information Protection Principles and Health Privacy Principles when collecting, storing, accessing and using personal and health information.

### 4.4 Risk Based Continual Improvement Approach

Council takes a risk based, continual improvement approach to protect the confidentiality, integrity and availability of the information it holds. Effective breach management, including notification where warranted, assists Council in avoiding or reducing possible harm to both the affected individuals / organisations and Council.

### 4.5 Preparedness and Contingency Measures

Council has implemented a Data Breach Response Plan to assist in responding to suspected data breaches with the aim of preventing data breaches in the future.

In the event of a suspected data breach, Council's Data Breach Response Team will undertake the following steps that form the Data Breach Response Plan:

1. Contain the Breach.

2. Assess and evaluate the associated risks.

3. Notify affected individuals / organisations where appropriate.

4. Review to prevent a repeat.

## 5. DATA BREACH RESPONSE PLAN

Suspected data breaches will be assessed on a case-by-case basis by undertaking an assessment of the risks involved to decide what actions to take under the circumstances. The Data Breach Response Plan specifies the requirements for:

- The Data Breach Response Team – membership and responsibilities.
- The steps to be taken in the event of a breach.

## 6. RESPONSIBILITIES

### 6.1 Responsible Officer

The Chief Information Officer is the Responsible Officer for this policy. These responsibilities include but are not limited to:

- Ensuring the Policy is current and in line with relevant legislation / policies.
- Providing a point of contact for anyone wanting information or advice about the meaning and application of the Policy.

### 6.2 Chief Executive Officer

The Chief Executive Officer has delegated the authority for the Chief Information Officer to exercise the responsibilities detailed in this Policy.

### 6.3 Directors

Directors are responsible for ensuring their Directorate adheres to the requirements of this Policy and provide guidance in respect of the correct handling of data within their division and the organisation.

### 6.4 Employees

An employee, contractor or volunteer who has identified a suspected data breach must immediately notify their Manager and the Privacy and Access to Information Officer (or equivalent).

Councillors must notify Council via the Corporate Governance team.

### 6.5 Privacy and Access to Information Officer (or equivalent)

The Privacy and Access to Information Officer (or equivalent) is responsible for:

- Ensuring the Data Breach Response Plan and associated response and escalation procedures are defined and documented to ensure the handling of data breach incidents is timely and effective.
- Leading the investigation of a suspected data breach incident and initiating the Data Breach Response Plan when needed.

### 6.6 Data Breach Response Team

Councill will assemble the Data Breach Response Team who will determine whether an eligible data breach has occurred. The Data Breach Review Team will take steps to:

- Perform activities as specified in the Data Breach Response Plan.
- Avoid or remedy any actual or potential harm.
- Report to the NSW Privacy Commissioner as necessary.

## 7. POLICY COMPLIANCE

This Policy complies with NSW Mandatory Notification of Data Breach (MNDB) scheme established by Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) effective 28 November 2023.

## 8. RECORD KEEPING, CONFIDENTIALITY AND PRIVACY

Council adheres to and complies with the *NSW State Records Act 1998* and *Privacy and Personal Information Protection Act 1998* through its Data Breach Notification Policy, Access to Information Policy and Privacy Management Plan.

## 9. BREACHES OF POLICY

Breaches of this Policy will be dealt with in accordance with relevant legislation and will be advised to the Chief Executive Officer and / or Director Corporate Support via the Chief Information Officer where appropriate.

## 10. RELATED DOCUMENTS

- Council's Agency Information Guide.
- Code of Conduct for Council Staff.
- Code of Conduct for Councillors.
- Privacy Management Plan.

- Customer Feedback and Complaints Management Policy.
- Cyber Security Policy.

## 11. RELEVANT LEGISLATION AND REGULATIONS

- *Government Information (Public Access) Act 2009 (NSW)*
- *Government Information (Public Access) Regulation 2018 (NSW)*
- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Heath Records and Information Privacy Act 2002 (NSW)*
- *State Records Act 1998 (NSW)*
- *Local Government Act 1993 (NSW)*
- *Children (Education and Care Services National Law Application) Act 2010 (NSW)*
- *Education and Care Services National Regulations (NSW)*
- *Environmental Planning & Assessment Act 1979 (NSW)*
- *Public Interest Disclosures Act 1994 (NSW)*
- *Data Sharing (Government Sector) Act 2015 (NSW)*
- *Copyright Act 1968*

## 12. DEFINITION OF TERMS

| Term | Meaning |
|---|---|
| Eligible Data Breach | Occurs when there is:<br><br>Unauthorised access, unauthorised disclosure or loss of personal or health information held by an agency where the loss is likely to result in unauthorised access or disclosure; and<br><br>A reasonable person would conclude that this would be likely to result in serious harm to an individual to whom the information relates. |

End of Document



| | | | |
|---|---|---|---|
| **UNCONTROLLED COPY WHEN PRINTED -** For up to date copy please refer to Sutherland Shire Council Intranet / Website | | | |
| **Document Name**: Data Breach Notification Policy | | **Policy Accountability** Chief Information Officer | |
| **Version**: #1.0 | **Approved by**: Council (GOV010-24) | **Minute No:** 41 | **Date approved:** 18/03/2024 |
| **Original:** March 2024 | **Last Revision**: March 2024 | **Next Revision**: February 2026 | |