DATA BREACH NOTIFICATION POLICY

March 2026

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.

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).

2. APPLICATION

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

3. PRINCIPLES

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

4. 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.

5. RESPONSIBILITIES

4.1 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.

4.2 Chief Executive Officer

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

4.3 Directors

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

4.4 Employees

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

Councillors must notify Council via the Corporate Governance team.

4.5 Privacy and Information Management Lead (or equivalent)

The Privacy and Information Management Lead (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.

4.6 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.

6. 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.

7. 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.

8. 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 via the Chief Information Officer where appropriate.

9. 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

10. 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 and Assessment Act 1979 (NSW)*
- *Public Interest Disclosures Act 1994 (NSW)*
- *Data Sharing (Government Sector) Act 2015 (NSW)*
- *Copyright Act 1968*

11. DEFINITION OF TERMS

Term	Meaning
Eligible Data Breach	Occurs when there is: 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 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: 2	**Approved by**: Council (COR006-26)	**Minute No:** 52	**Date approved:** 23/03/2026
Original: October 2023	**Last Version**: March 2024	**Next Revision**: March 2029	

SCHEDULE TO DATA BREACH NOTIFICATION POLICY

1. PURPOSE

The purpose of this Guideline is to provide guidance in relation to the required steps for implementing Council's Data Breach Policy.

This guideline serves as Councils Data Breach Response Plan for responding to a data breach and aligns with the NSW Mandatory Notification of Data Breach Scheme ('MNDB Scheme').

This Guideline assists Council and its employees to respond timely and effectively to a data breach. Effective Data Breach response is key to avoiding and / or reducing possible harm to affected individuals, organisations and Council. and it also provides the opportunity for lessons to be learned which may prevent future breaches.

2. MANDATORY REPORTING

The MNDB Scheme is a mandatory reporting requirement under the *Privacy and Personal Information Protection Act 1998* for NSW public sector agencies ('agencies') in the event of an 'eligible data breach'.

2.1. Notifying The NSW Privacy Commissioner

Council must notify the NSW Privacy Commissioner immediately of an eligible data breach using the form on the Information and Privacy Commission NSW (IPC) website.

In some circumstances, it may be obvious an eligible data breach has occurred before a full assessment is completed and Council should notify the NSW Privacy Commissioner at this time.

Council should keep the NSW Privacy Commissioner updated as the breach response progresses, and new information is known.

2.2. Public Notification Register

A public notification register must be published on Council's website for notifications made by way of public notice.

A public notification must be publicly available for at least 12 months and contain information that would be included in a direct notification to affected individuals / organisations with the exclusion of personal information on an individual and / or information considered confidential and would prejudice Council's functions.

In addition to publishing notifications, Council must take reasonable steps to publicise the contents of the notice to increase the likelihood of bringing it to the attention of individuals at risk of serious harm.

The NSW Privacy Commissioner must be advised how and where to access the published notification so it can be published on the Information and Privacy Commissioner (NSW) website.

2.3. Internal Incident Register

Council must maintain an internal register of eligible data breaches with information to be included where practicable:

- Who was notified of the breach.
- When the breach was notified.
- Details of steps taken by Council to mitigate any harm

- Details of the action taken to prevent future breaches.
- Estimated cost of the breach.

3. DATA BREACH RESPONSE

In the event of a suspected data breach the Privacy and Access to Information Officer (or equivalent) is responsible for managing and co-ordinating the Data Breach Response Plan and engaging the Data Breach Response Team.

3.1 Data Breach Response Team

Membership of the Data Breach Response (DBR) Team includes (but is not limited to):

Data Breach Response Team Role	Position	Responsibilities
Incident Response Lead	The Privacy and Information Management Lead	• Data Breach Response Co-ordination • Issuing required notifications
Technical Lead	Cyber Security and Risk Lead	• Breach assessment • Peer review • Liaison with Cyber Security Response Team
Member	Chief Information Officer	• Breach assessment • Resource mobilisation • Executive communications
Member	IMandT Service Centre Manager	• Breach assessment • Resource mobilisation

The DBR Team must assess and determine whether an eligible reportable data breach has occurred. Section 7 provides examples of data breaches.

An eligible data breach occurs when there is:

- 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
- A reasonable person would conclude that this would be likely to result in serious harm to an individual to whom the information relates.

There are four key steps to consider when responding to a breach or suspected breach and steps 1-3 should be carried out concurrently or in close succession.

Step One: Contain the Breach

Containing the breach is prioritised by Council. All possible necessary steps must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

If a third party is in possession of the data and declines to return it, it may be necessary for Council to seek legal or other advice on what action can be taken to recover the data. When recovering data, Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

Step Two: Assess and Evaluate the Associated Risks

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

Council must assess and determine whether the data breach is an eligible data breach within 30 days from the date they become aware of a possible data breach.

Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already incurred.

Factors Council will consider when deciding whether a data breach is an eligible data breach and if notification is appropriate include:

- Who is affected by the breach? Council will review whether individuals and organisations have been affected by the breach.
- How many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

What was the cause of the breach?

Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an inadvertent oversight. Was it a one-off incident? Has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the confidential information been recovered? Is the confidential information encrypted or otherwise not readily accessible?

What is the risk of harm to the affected individuals / organisations?

Assessment will include reviewing what possible use there is for the confidential information while considering the sensitivity of the type of information (such as Health Information, Personal Information subject to special restrictions under s.19(1) of the *Privacy and Personal Information Protection Act 1998*) which could be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the information? What is the risk of further access, use or disclosure, including via media or online? Does it risk embarrassment or harm to stakeholders and / or damage Council's reputation?

Step Three: Notifying Affected Individuals / Organisations

Council recognises that notification to individuals / organisations affected by a data breach can assist in mitigating any damage for those affected individuals / organisations. Notification demonstrates a commitment to open and transparent governance, consistent with Council's approach.

Obligations under the MNDB Scheme require Council to notify affected individuals where a data breach is assessed as an eligible data breach.

When to notify affected individuals / organisations

In situations when notification is required it should be done promptly to assist in avoiding or lessening any potential damage by enabling the individual / organisation to take steps to protect themselves.

Individuals / organisations affected by an eligible data breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or publicly reveal a system vulnerability.

Once Council has determined that an eligible data breach has occurred, Council must notify certain individuals as soon as practicable.

There are three options for notifying individuals that are affected by a breach.

1. Only individuals at risk of serious harm.
2. All individuals whose information was compromised.
3. Public notification.

Council is not required to notify individuals / organisations of an eligible data breach if an exemption applies. However, Council is still required to notify the NSW Privacy Commissioner.

Examples of exemptions include:

- Breaches involving multiple agencies.
- Investigations and legal proceedings.
- Mitigation of harm.
- Secrecy provisions.
- Serious risk of harm to health or safety.
- Increased risk to cyber security.
- Further guidance on exemptions can be found here

How to notify affected parties

The method of notifying affected individuals/organisations will depend on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Affected individuals / organisations should be notified directly – by telephone, letter, email or in person.

A Public notification posted on the Council's website, in a newspaper, or a media release should only occur where the contact information of affected individuals / organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm.

What to include in the notification

The notification to affected parties must include information about the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.

The notification advice will be tailored to the circumstances of the breach. Content of a notification could include:

- Information about the breach, including when it happened.
- A description of what confidential or personal information has been disclosed.
- What the Council is doing to control or reduce the harm.
- What steps the person / organisation can take to further protect themselves and what Council will do to assist in doing this.
- Contact details for questions or requests for information.
- The right to lodge a privacy complaint with the NSW Privacy Commissioner.

Step Four: Review to Prevent a Repeat

Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- Security audit of both physical and technical security controls.
- Review of policies and procedures.
- Review of staff / contractor training practices.

4. EXAMPLE OF DATA BREACHES

The table below shows examples of data breaches by cause and may assist the DBR in breach assessment.

Human Error	• When a letter or email is sent to the wrong recipient. • When system access is incorrectly granted to someone without appropriate authorisation. • When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced. • When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information.
System Failure	• Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients. • Where systems are not maintained through the application of known and supported patches.
Malicious or Criminal Attack	• Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information. • Social engineering or impersonation leading into inappropriate disclosure of personal information. • Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions. • Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

5. RECORD KEEPING REQUIREMENTS

The DBR Team will record:

- The description of the breach or suspected breach.
- The action taken to address the breach or suspected breach.
- The outcome of that action.
- Steps taken to date to avoid or remedy any actual or potential harm.
- Confirmation that the incident has been recorded on the public Data Breach Notification Register where applicable.
- Confirmation that the incident has been recorded on the internal Incident Register where applicable.
- Confirmation that the incident has been reported to the NSW Privacy Commissioner.

End of Document

UNCONTROLLED COPY WHEN PRINTED - For up to date copy please refer to Sutherland Shire Council Intranet / Website			
Document Name: Schedule to Data Breach Notification Policy		**Schedule Accountability** *[role of accountable officer]*	
Version: 1	**Approved by**: Council (COR006-26)	**Minute No:** 52	**Date approved:** 23/03/2026
Original: March 2026	**Last Version**: N/A		**Next Revision**: March 2029