Policy Owner: **Director Corporate Services**

Direction: **5. Our Civic Leadership**

1. STATEMENT OF INTENT

This Policy provides guidance to Council officers in responding to a Data Breach. This Policy arises principally of Council's responsibilities in respect Privacy Legislation. The Policy responds to Council's aim to provide services to its community in a manner that respects security of Personal Information.

2. ELIGIBILITY

This Policy applies to a Data Breach. The Policy applies to all Workers and external organisations who have access to Council's infrastructure, services, and data.

3. INTEPRETATION

3.1 Defined terms

First letter capital format is used for defined terms. For defined terms refer to section 4. Definitions.

4. DEFINITIONS

Terms used in the Policy have the following meanings:

Term	Definition
Complaint	Complaint is defined in the Complaints Handling Policy.
Council	North Sydney Council
Data Breach	An incident, in which: • Personal Information, or, • Health Information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen, or used by unauthorised individuals, whether accidentally or intentionally. A data breach may involve either electronically formatted data or data held in hard copy.
Data Breach Response Team	Appropriately skilled team entrusted to respond to Data Breach incidents.

Term	Definition
Eligible Data Breach	Eligible Data Breach is defined in legislation as: • in section 59D(1) Meaning of eligible data breach and affected individual of Privacy and Personal Information Protection Act 1998 (NSW), or, • in 26WE Eligible Data Breach of Privacy Act 1988 (Cth) and is addressed in this Policy as relevant to the Eligible Data Breach. A Data Breach of Health Information is subject the Eligible Data Breach provisions of the Privacy and Personal Information Protection Act 1998 (NSW).
Health Information	The definition of health information is provided in Section 6 of the Health Records and Information Privacy Act 2002 (NSW)
Malware	As defined in the Cyber Security NSW Glossary
Personal Information	Personal information is defined in legislation as: • in section 4 Definition of "Personal Information" of Privacy and Personal Information Protection Act 1998 (NSW), or, • in section 5 Definition of "Personal Information" of Health Records and Information Privacy Act 2002 (NSW), or, • in section 6(1) Interpretations of Privacy Act 1988 (Cth) and is addressed in this Policy as relevant to the Data Breach.
Privacy Impact Assessment	Is defined in the Privacy Impact Assessment Guide issued by the NSW Information Privacy Commissioner.
Privacy Legislation	<u>NSW legislation</u> Privacy and Personal Information Protection Act 1988 (NSW) Health Record and Information Privacy Act 2002 (NSW) <u>Commonwealth legislation</u> Privacy (Tax File Number) Rule 2015 established of the Privacy Act 1988 (Cth) Usually, this Policy will practically respond to NSW legislation. The Commonwealth legislation only applies in a limited number of instances such as arises of tax file numbers.
Ransomware	As defined in the Cyber Security NSW Glossary
Workers	Council councillors, employees, contractors, students, volunteers, and agency personnel.

5. PROVISIONS

5.1 Examples of a data breach?

Examples of Data Breaches include:

- information mistakenly given to the wrong person (for instance by means of attachment of an incorrect attachment to an email);
- accidental loss or theft of a device that stores data (e.g., loss of paper record, laptop, iPad, or USB stick);
- unauthorised access to an electronic database by a rogue actor;
- a system failure, or breach of physical security, which results in unwanted access to information;
- unauthorised use, stolen or hacked credentials leading to a breach, access to or modification of data or information systems (e.g., sharing of user login details (deliberately or accidentally) to gain unauthorised access or making unauthorised changes to data or information systems);
- data leakage from failing to meet Payment Card Industry Data Security Standards;
- malware or ransomware.

Council is aware that most data breaches arise of human error and only some instances of Data Breach are Eligible Data Breach.

5.2 When does Council know a Data Breach has occurred?

Council awareness of a Data Breach may arise through:

- an alert raised through Council's security systems,
- a notification from a member of staff,
- a notification from a contractor,
- a notification from an affected third party, or,
- through receipt of a report from another government agency.

Council may also receive a Complaint that identifies a Data Breach incident. In such instances the Worker assigned to handling the Complaint will maintain independence of any Workers that investigate, and/or respond to the Data Breach.

Council will make means available to raise notifications of Data Breach through our email address, council@northsydney.nsw.gov.au, or through our General Enquiry online form on our website. These will be routed to Workers who investigate, and/or respond to the Data Breach.

5.3 Acknowledgment of Data Breach notification schemes

Council acknowledges, and commits to meet the responsibilities arising of schemes that require notification when an Eligible Data Breach is detected.

NSW scheme

A Mandatory Notifiable Data Breach scheme applies to an Eligible Data Breach.

Commonwealth scheme

A Notifiable Data Breaches scheme applies to an Eligible Data Breach.

6. HOW HAS COUNCIL PREPARED FOR POTENTIAL DATA BREACHES?

6.1 Training and awareness

As part of induction training, Council staff will undertake cyber security training. As an ongoing measure to ensure staff awareness, Council conducts regular cyber security training to all staff on topics such as:

- credential harvesting,
- business email compromise, and
- ransomware.

Exercises conducted in-house once a year simulate:

- an information technology security attack, and,
- a disaster recovery.

6.2 Appropriate ongoing monitoring of data security on infrastructure; both hosted and in-house

Council deploys an active cyber security system with real-time alerts. Response to alerts from the system arise both in real-time and through escalation.

6.3 Contractual arrangements

Agreements that Council form with contractors that access Council's network infrastructure, services, or data, include clauses that contractually bind the contractor to:

- notify Council of a Data Breach, and,
- assist Council to contain, investigate and report a Data Breach.

A supplier may also need to report an Eligible Data Breach in accordance with the Commonwealth Privacy Legislation while at the same time Council is reporting the same Eligible Data Breach as to the State Privacy Legislation. During times of tender evaluation and contract formation, Council will exercise scrutiny, including Privacy Impact Assessment, in evaluation of a contractor's preparedness for data security and reporting of an Eligible Data Breach.

6.4 Schedule for testing and updating this policy

This policy will be formally reviewed every two years to ensure it is fit for purpose. Additionally, further changes to this Policy may be determined as an outcome of the review and prevent assessment conducted for individual breaches.

7. DATA BREACH RESPONSE PROCESS

7.1 Data Breach preparedness

Council's Information Technology network and infrastructure is managed in-house, and cyber-security measures are maintained to ensure cyber-security maturity. Such measures include:

- a cyber-security event management system,
- A Crisis Plan covering disaster recovery and business continuity plans,
- information Technology network segment design, and,
- information access controls.

Council's Information security processes also include numerous other measures including physical security and information handling policies in pursuit of data security. The information security processes include controls that impose security classifications upon data such that the number of personnel that can access certain data is limited.

7.2 Co-operation with other agencies

Council will co-operate with all other governmental agencies; State and Commonwealth; Regulators, Crime enforcement, and Cyber-Security, on both:

- acting on notifications of Data Breaches affecting Council, and,
- acting to assist (where possible of Council's Privacy Management Plan) in the resolution of Data Breaches affecting other entities.

The Council's Public Officer is responsible for ensuring co-operation with other governmental agencies.

7.3 Data Breach Response Plan

Council's Data Breach Response Plan documents Council's operational response to a Data Breach and establishes the responsibilities and procedures to be taken by those who hold responsibility following a Data Breach. The response plan includes a process for identifying and addressing the root cause(s) that contributed to the Data Breach.

Council's Data Breach Response Plan also documents Council's operational response to an Eligible Data Breach and establishes the responsibilities and procedures to be

taken by those who hold responsibility following an Eligible Data Breach. Council's Data Breach Response Plan identifies Council's obligation to:

- immediately make all reasonable efforts to contain a Data Breach,
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an Eligible Data Breach,
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected Data Breach,
- decide whether a Data Breach is an Eligible Data Breach or there are reasonable grounds to believe the Data Breach is an Eligible Data Breach.
- notify the NSW Privacy Commissioner and affected individuals of the Eligible Data Breach using the Data Breach Notification to the Privacy Commissioner form,
- comply with other data management requirements.

7.4 Communication Strategy

If during the initial assessment the Privacy Officer determines the Data Breach to be an Eligible Data Breach, the Privacy Officer must give immediate notification to the NSW Privacy Commissioner, or Office of Australian Information Commissioner, as applicable, and, except if exempted under Part 6A, Division 4 of Privacy and Personal Information Protection Act 1988 (NSW) or Privacy Act 1988 (Cth) section 26WF, all affected individuals as soon as practicable after Council becomes aware of the Eligible Data Breach. Such notifications will have regard of both this Policy and Council's Privacy Management Plan.

Where a Data Breach is made apparent to Council through a Complaint, the affected individual will be offered information as soon as practical to assist the affected individual in their understanding of the information that was subject to the Data Breach.

Where Council needs additional time to investigate a Data Breach, or to engage professional support, Council will ensure that a final report follows an initial notification of a Data Breach that summarises Council's findings and actions taken to address.

Council will hold a register of all Data Breaches and Eligible Data Breaches. All public notifications for Eligible Data Breaches made in the previous twelve months will be published on Council's website in a publicly available register.

In the event of a Data Breach, Council will issue a statement on our website to notify the public. The notification will include, as relevant:

- Brief details of the nature of the Data Breach, including:
    - Date of detection of the Data Breach,

  - An initial estimate of the number of individuals impacted by the Data Breach,
- An indication of initial containment activity,
- An indication of which authorities the breach has been reported to,
- Contact details of Council,
- An indication of when individuals impacted by the Data Breach will be contacted, and,
- An indication of how the individuals impacted by the Data Breach will be contacted.

The notification is not to indicate whether the Data Breach is an Eligible Data Breach. Council will not engage any media in notification of a Data Breach other than in response to media enquiries arising from the statement placed upon Council's website.

7.5 Insurance

Council will ensure that it holds appropriate insurances to respond to Data Breach losses.

8. RESPONSIBILITY/ACCOUNTABILITY

Position	Responsibilities
Members of the Data Breach Response Team	
Director Corporate Services	General governance, compliance and records management advice and coordination of preliminary assessment and Data Breach Response Team.
Chief Information Officer	Responsibility for the overall governance of security for all IT systems.
Team Leader Application Services	Provide advice around application level data/information security.
Team Leader Digital Platforms	Provide advice around technical/IT infrastructure security.
Service Unit Manager, Customer and Communications	Communications advice, including notification to affected individuals for "Eligible Data Breach".
Invitees to the Data Breach Response Team	
General Counsel	Legal and Insurance advice
Privacy Contact Officer	Determination of "Eligible Data Breach" Privacy advice and logging of all breaches. Maintain digest on Council's webpage.
Chief Financial Officer	Payment Card Industry Data Security Standard and general advice.
Chief Executive Officer (High Risk Only)	Overall accountability as per Local Government Act 1993 (NSW).

The Data Breach Response Team is an occasional team. The Director Corporate Services convenes the team in response to a Data Breach incident. The Data Breach Response Team may seek advice from third party privacy specialists, NSW Information and Privacy Commission, Office of Australian Information Commissioner or Cyber Security NSW (of the Commonwealth agency of equivalence to the Cyber Security NSW) if deemed necessary as part of the assessment process.

The Data Breach Response Team operates to the Data Breach Response Team Terms of Reference.

It is recognised that the Privacy Officer may have a primary role in handling a Complaint. When handling a Complaint that has identified a Data Breach, the Privacy Officer will maintain their independence of the Data Breach Response Team.

9. DATA BREACH ESCALATION

9.1 Response escalation

Data Breach incidents will be assessed according to the type of information accessed, the potential impact and the initial review of the points of failure leading to the incident by the Data Breach Response Team.

This will determine the various levels of resource, reporting and external contacts required for each incident type.

9.2 Reporting

The Data Breach Response Team completes the reporting of a Data Breach. The report format is included in the Data Breach Response Plan.

10. RELATED POLICIES/DOCUMENTS/LEGISLATION

This Policy reads in conjunction with the following Council policies and documents:

- Complaints Handling Policy
- Crisis Plan
- Data Breach Response Plan
- Data Breach Response Team Terms of Reference
- Information Security Incident Management Policy (ISMS-POL-003)
- Information Security Incident Management Plan (ISMS-STD-004)
- Information Security Access Policy (ISMS-POL-002)
- Privacy Management Plan

This Policy reads in conjunction with the following documents/legislation:

- Privacy Act 1988 (Cth)
- Health Record and Information Privacy Act 2002 (NSW)
- Privacy and Personal Information Protection Act 1988 (NSW)

Version	Date Approved	Approved by	Resolution No.	Review Date
1	4 July 2024	ELT	na	2026/27