Data Breach Policy & Response Plan

Adoption Date:	1 March 2024 by Approval of the General Manager – PUBLIC VERSION
Last Reviewed:	April 2024
Next Review Date:	February 2025
Division/Department:	Corporate Performance / Information & Digital Transformation / Governance
Responsible Officer:	Manager Governance & Risk
HPE CM Record Number:	

1 Policy Statement

Part 6A of the Privacy and Personal Information Protection Act 1998 (PPIP Act) establishes the NSW Mandatory Notification of Data breach (MNDB) scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches. Under the scheme, public sector agencies (such as Woollahra Municipal Council) are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches.

This Policy will assist Council to meet its legal obligations in respect of the MNDB under the PPIP Act and Privacy Act 1988.

2 Application

Purpose

The purpose of this policy is to provide guidance to Council staff in responding to a breach of Council held data, particularly as it relates to personal information.

This policy also provides the community with an understanding of how Council will manage a data breach of Council held data, plus the policy sets out Council's response plan for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach.

Effective data breach management, including notification where warranted, assists Council in avoiding or reducing possible harm to both the affected individuals / organisations and Council, and may prevent future breaches.

The policy sets out Council's approach to identifying and managing a data breach, including:

- Providing examples of situations considered to constitute a data breach;
- The five key steps involved in responding to a data breach;
- The considerations around notifying persons whose privacy may be affected by a data breach on a mandatory basis where required, or on a voluntary basis where warranted, to ensure that the Council responds appropriately to a data breach;
- Reporting requirements.

Scope

This policy applies to all Councillors, Council staff and contractors of Council. This includes temporary and casual staff, private contractors and consultants engaged by Council to perform the role of a public official.

3 Quick Reference Guide

It is acknowledged that this policy contains a considerable amount of detail relating to data breaches and related processes. Therefore, in order to ensure Council staff have ready access to key information as included in this policy, this quick reference guide has been developed. It should be noted that this quick reference guide is not a substitute for the full detailed information contained within this policy, but is here to assist staff in navigating their way through the policy.

The most important and immediate information for all staff to take note of is this:

Who to contact if you suspect a data breach?

Your immediate contact should be:

Jennifer Chenhall
Manager Governance & Risk (Privacy Officer / Assessor)

Email: jennifer.chenhall@woollahra.nsw.gov.au

Phone: **02 9391 7012**
Mobile: [redacted]

You must then inform your **Manager** and your **Director**

Refer to **Section 11** of this policy for more information, as well as **Attachment A**.

Here is a further quick reference guide to other key parts of this policy:

The What?	Where to find it:
Definitions	Refer to **Section 4**
Contact Details	Refer to **Section 5** Key contact details are included in **Section 5** along with key roles and responsibilities.
What is a data breach?	Refer to **Section 6**: A data breach is an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by (or on behalf of) Council.
Examples of a data breach	Refer to **Section 6**: - A cyber-attack resulting in potential or actual access or extraction of personal information - The loss of a Council owned device containing personal information and the potential or actual access or extraction of personal information contained within it (e.g. a laptop or iPad) - The distribution of personal information through methods such as email or file sharing services e.g. the accidental emailing of a spreadsheet with payroll and bank account details
What is personal information?	Refer to **Section 7**: - Employee information - this could include Tax File Numbers (TFN's), bank account and salary information, home addresses, superannuation details, date of birth, next of kin and medical related records.

The What?	Where to find it:
	- Customer information including residents, ratepayers and users of Council facilities and services i.e. Libraries. This could include bank accounts, home addresses, email addresses, service usage information and phone numbers.
Role, Responsibilities and Contact List	Refer to **Section 5** Key contact details are included in **Section 5** along with key roles and responsibilities
Who to contact if you suspect a data breach?	Refer to **Section 11** and the flow chart: Your immediate contact should be as follows: **Jennifer Chenhall** Manager Governance & Risk Email: jennifer.chenhall@woollahra.nsw.gov.au Phone: **02 9391 7012** Mobile: [redacted] Your Manager Your Director

4 Definitions

Term	Meaning
Affected Individual	An “affected individual” as defined in the PPIP Act.
Assessor	The Manager Governance & Risk (Manager G&R) or alternatively known in this policy as the Privacy Officer.
Commonwealth Notifiable Data breach	An “eligible data breach” as defined in the Privacy Act.
Contractor	A third party provider of goods or services to Council.
Council Held Information	Any personal information in whatever form (including hard copy and electronically held information), which is held by Council or is otherwise in the possession or control of Council.
Council Official	As defined in Part 2 of the Woollahra Council Code of Conduct, includes Councillors, members of staff of Council, administrators, Council committee members, delegates of Council and for the purposes of clause 4.16 of the Code of Conduct, Council advisers.
Council Officer	Any officer or employee of Council, including temporary and casual staff.
Data breach	A data breach is an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by (or on behalf of) Council.
Data Breach Response Team (DBRT)	The team established for the purposes of responding to a data breach that as a minimum includes the General Manager, Director Corporate Performance (DCP), Manager Governance & Risk

Term	Meaning
	(MG&R), Manager Information & Digital Transformation (MI&DT) and Manager Communications & Engagement (MC&E).
Eligible Data Breach	An 'eligible data breach' is defined in section 59D of the PPIP Act to mean: 1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and 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, or 2. Personal information held by a public sector agency is lost in circumstances where: (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates For further information, please refer to Clause 5 of this policy.
Health Information	As defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act), health information means: 1. personal information that is information or an opinion about (i) the physical or mental health or a disability (at any time) of an individual, or (ii) an individual's express wishes about the future provision of health services to him or her, or (iii) a health service provided, or to be provided, to an individual, or 2. other personal information collected to provide, or in providing, a health service, or 3. other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or 4. other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or 5. healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act. For the purposes of this Policy, personal information includes health information.
HRIP Act	The *Health Records & Information and Privacy Act 2002* (NSW).
IPC	The Information and Privacy Commission of NSW.
OAIC	The Office of the Australian Information Commissioner.

Term	Meaning
MRDB	A Mandatory Reporting Data Breach is an Eligible Data Breach or a Commonwealth Notifiable Data breach.
MNDB	The Mandatory Notification of Data Breach Scheme, which requires Council to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm. Please see the IPC notification form at **Attachment E**.
Non-Eligible Data breach	Any data breach that is not a Mandatory Reporting Data Breach.
Personal Information	Any information defined as "personal information" under the Privacy Act, PPIP Act, or "health information" under the HRIP Act. In relation to the PPIP Act, personal information can include: Employee information including prospective, current and former employees. This could include Tax File Numbers (TFN's), bank account and salary information, home addresses, superannuation details, date of birth, next of kin and medical related records. Customer information including residents, ratepayers and users of Council facilities and services i.e. Libraries. This could include bank accounts, home addresses, email addresses, service usage information and phone numbers. Councillor information including prospective, current and former councillors. This could include Tax File Numbers (TFN's), bank account information, home addresses, superannuation details, date of birth, and financial information. For further information, please refer to **Section 7**.
PPIP Act	The *Privacy and Personal Information Protection Act 2022* (NSW).
Privacy Act	The *Privacy Act 1988* (Cth).
Privacy Commissioner	The NSW Privacy Commissioner, or as otherwise defined in the PPIP Act.
Privacy Officer	The Manager Governance & Risk.
Relevant Manager or Director	The Manager or Director to whom a Council Officer reports, or the Manager or Director with responsibility for a contract with a third party contractor.
Serious Harm	Harm arising from a data breach that has or may result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.
TFN	Is a Tax File Number as defined in Part VA of the *Income Tax Assessment Act 1936* (Cth).
Threat Actor	A malicious entity or individual that is partially or wholly responsible for an incident that impacts, or has the potential to impact, an organisation's security.

5 Roles, responsibilities & contact details

Role	Responsibilities
All Staff	- All staff are required to have read this policy. - Comply with the PPIP and HRIP Acts including protecting personal information held by the Council from unauthorised access, disclosure or loss, to the best of their ability. - Maintain electronic devices in accordance with the Policies of Council. - Report any suspected data breach including facts, documents and any other relevant information, in line with the requirements detailed in this Policy. - Promptly respond to requests for information from the Assessor or any member of the DBRT or your Manager and or Director.
Assessor (Also known as the Privacy Officer and / or Manager Governance & Risk) **Jennifer Chenhall** **Manager Governance & Risk** Email: jennifer.chenhall@woollahra.nsw.gov.au Phone: **02 9391 7012** Mobile: [redacted]	- Delegated by the General Manager to conduct assessments in accordance with Part 6A of the PPIP Act and is therefore the primary assessor. - On being alerted to a data breach, immediately notify the General Manager (or their delegate). - Carries out the risk assessment of the data breach in a timely and effective manner and prepares a report using agree template/s. - Provides advice and recommendations to the General Manager on the need to constitute the Data Breach Response Team (DBRT) in one or more of the following circumstances and in accordance with this policy: o If the risk severity rating is medium or above o If the data breach is considered to be a cyber-security incident i.e. a malicious or criminal attack o Data has likely been breached that is highly confidential or the release of which may lead to serious harm o Significant community interest - Consult with internal and external stakeholders as required i.e. insurers, legal advisors, Police, IPC, OAIC and the NSW Department of Customer Service (Cyber Security NSW). - Seek guidance from third party experts as required. - Provides a recommendation to the General Manager as to whether it is an Eligible Data Breach. - Manages the notification to affected individuals (as applicable) following the approval of the General Manager. - Reviews and reports actions to the General Manager and the DBRT (if constituted). - Prepares a confidential data breach review report for each separate data breach incident, for submission to the Executive Leadership Team, post the incident, using an agreed report template. - Follow this policy when responding to a data breach. - Oversees the implementation of agreed actions and recommendations in follow up to a data breach incident. - Manages the establishment and ongoing maintenance of the Public Notifications Data Breach Register on Council's website. - Maintains an internal Eligible Data Breach register. - Maintains all required information relating to data breaches on Councils web site. *Note: A person who is reasonably suspected as being involved in an action or omission that led to the data breach is not permitted to be an assessor.*

Role	Responsibilities
Director Corporate Performance (DCP) **Sue Meekin** **Director Corporate Performance** Email: Sue.meekin@woollahra.nsw.gov.au Phone: **02 9391 7014** Mobile: [redacted]	- Alternate Assessor and member of the DBRT.
Data Breach Response Team (DBRT)	- Once constituted by the General Manager, assemble promptly to review and respond to a data breach incident. - Review the Assessor's or the Manager I&DT's preliminary assessment of the data breach. - The DBRT will include as a minimum the General Manager, Director Corporate Performance, Manager Governance & Risk, Manager Information & Digital Transformation and the Manager Communications & Engagement (MCE) and the relevant Manager and or Director responsible for the area of the organisation where the breach occurred. - Investigate the data breach using the five step process outlined in this policy. - Determine whether Council's Business Continuity Plan needs to be activated, particularly if IT systems have to be shut down/off-line for any significant period of time.
General Manager **Craig Swift-McNair** **General Manager** Email: Craig.swift-mcnair@woollahra.nsw.gov.au Phone: **02 9391 7010** Mobile: [redacted]	- Ensure Council complies with the MNDB Scheme. - Determines if an Eligible Data Breach has occurred in accordance with the PPIP Act - Delegates an Assessor (Manager G&R) to lead the investigation under Section 59G of the PPIP Act. - Has the ability to approve an extension of the assessment period as per Section 59K of the PPIP Act, as the Head of Agency. - Notifies the IPC of an Eligible Data Breach. - Has the ability to approve an exemption under Division 4 of the PPIP Act. - Review and approve actions and recommendations in data breach reports. - Responsible for internal and external communication relating to any data breach to ensure a single source of truth for messaging. - Responsible for informing the Councillors and the Audit, Risk & Improvement Committee (ARIC) of any medium to high risk data breaches and the processes being undertaken to manage the incident.
Manager Communications & Engagement (MCE) **Justine Henderson** **Manager Communications & Engagement** Email: Justine.henderson@woollahra.nsw.gov.au Phone: **02 9391 7141** Mobile: [redacted]	- Liaise with the General Manager on internal and external communications relating to any data breach, to ensure a single source of truth for messaging. - Coordinate release of information on Council's website and media / press release as deemed appropriate by the General Manager and or Council's legal advisors and in accordance with the information included in this Policy. - Oversee any formal notifications to Affected Individuals required as a result of a data breach.

Role	Responsibilities
Manager Information & Digital Transformation (MIDT) **Ben Horn** **Manager Information & Digital Transformation** Email: Ben.horn@woollahra.nsw.gov.au Phone: **02 9391 7088** Mobile: [redacted]	- If it is considered that a data breach is the result of a cyber-security incident i.e. a malicious or criminal attack, then do what is required to contain the breach and maintain the integrity of other Council systems. - If the breach relates to Information Technology or Information Management, investigate the breach in a timely and effective manner, in coordination with the Assessor. - In the event of a cyber-security incident, coordinate immediate remedial actions as required by the Assessor and or third party agencies. - Prepare relevant information on the data breach (including proposed actions and recommendations) and provide this to the Assessor in order for the Assessor to be able to draft a report to provide to the General Manager (or the DBRT if constituted) for consideration. - Assessment of the impact of the cyber-security incident.

6 What is a data breach?

A **data breach** is defined as:

An incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Council.

The MNDB scheme applies to breaches of 'personal information' as defined in the PPIP Act.

A data breach may be deliberate or accidental and may occur by a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive systems, inadvertent disclosure, social engineering or hacking.

Examples of data breaches that might occur in Council's context are:

- A cyber-attack resulting in potential or actual access or extraction of personal information (e.g. a threat actor / malicious actor manipulates a Council online service to access other resident accounts either individually or in bulk).

- The loss of a Council owned device containing personal information and the potential or actual access or extraction of personal information contained within (e.g. a laptop or iPad containing locally stored email messages relating to residents or employees).

- The distribution of personal information through methods such as email or file sharing services, including both malicious and / or accidental actions (e.g. the accidental emailing of a spreadsheet with payroll and bank account details, or the deliberate downloading of resident documents to a personal email account).

- The access or extraction of personal information for unauthorised purposes by those trusted with access to that information (e.g. a staff member looking up a person's home address or contact details for non-work purposes).

The MNDB does not apply to data breaches that do not involve personal information or health information or to breaches that are not likely to result in serious harm to an individual.

Where the scheme does not apply, Council is not required to mandatorily notify individuals or the Information and Privacy Commission (IPC), however it will be at the discretion of the General Manager as to what actions will be taken to respond to the breach. Council may at the discretion of the General Manager, still provide voluntary notification to the IPC and individuals where deemed appropriate.

7 What is an eligible data breach?

An **eligible data breach** as defined in s59D of the PPIP Act occurs when:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are 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.

In a Council context, personal information could include, but is not limited to:

3. Employee information including prospective, current and former employees. This could include Tax File Numbers (TFN's), bank account and salary information, home addresses, superannuation details, date of birth, next of kin and medical related records.

4. Customer information including residents, ratepayers and users of Council facilities and services i.e. Libraries. This could include bank accounts, home addresses, email addresses, service usage information and phone numbers.

5. Councillor information including prospective, current and former councillors. This could include Tax File Numbers (TFN's), bank account information, home addresses, superannuation details, date of birth, and financial information.

6. Audit, Risk & Improvement Committee member's information including prospective, current and former independent members. This could include Tax File Numbers (TFN's), bank account information, home addresses, superannuation details, date of birth, and financial information.

7. Local Planning Panel member's information, which could include TFN's, bank account information, home addresses, superannuation details, date of birth, and financial information.

8. CCTV information including the capture, storage and dissemination of images of persons (both in still and / or video format).

9. Motor Vehicle information in connection with enforcement of local laws including vehicle owner personal information.

10. Companion Animal ownership information including home addresses, email addresses and phone numbers.

What is <u>not</u> an eligible Data breach?

A data breach is not an eligible data breach if:

- It does not contain personal information, or
- Does not contain health information, or
- Is not likely to result in serious harm to an individual.

Where a data breach is not assessed to be an eligible data breach, Council is not required to mandatorily notify individuals or the IPC. However, Council must still take action to resolve the data breach. Council may also (at the discretion of the General Manager), still provide voluntary notification to the IPC and individuals where deemed appropriate.

8 What is serious harm?

Serious harm in relation to the definition of an eligible data breach includes such things as serious physical, psychological, emotional, financial, or reputational harm. The meaning of 'likely' in relation to the definition of an eligible data breach (see Definitions above), means the risk of serious harm to an individual is more probable than not.

Breaches of personal data can result in significant harm, including people having their identities stolen or the private home addresses of protected or vulnerable people being disclosed or compromised. In some circumstances, this can expose an individual to a significant risk of harm. As such, even a breach affecting a small number of people may have a large impact.

Serious harm in relation to a data breach could include:

- Risk to an individuals' safety
- Risk of identity theft
- Financial loss to an individual or organisation
- Damage to personal reputation or position
- Humiliation, embarrassment or bullying
- Damage to reputation or defamation.

It should be noted that Council's notification obligations under the relevant legislation may be triggered even if only one person is likely to suffer serious harm as a result of a data breach.

9 Steps taken to prepare for a data breach

Council maintains an effective and integrated risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation. Please refer to Council's Risk Management Policy & Framework for further information.

Council also has a range of supporting policies to control and mitigate exposures to breaches of data. This includes a Business Continuity Management Policy, a Fraud & Corruption Policy, Recruitment & Selection Policy and a Code of Conduct.

In addition to the above-mentioned policy controls, Council has a comprehensive set of Information Technology (IT) controls, processes and services designed to ensure that IT infrastructure, network, applications and information are monitored, maintained and secured. Council's IT staff, third-party providers and automated services routinely monitor, test, audit and enhance Council's IT environment and IT controls.

Council also continues to build a well-trained workforce with the focus being on:

- Enhancing staff awareness of privacy and cyber principles and current threat trends by providing training and awareness around identifying, responding to and managing data breaches.
- Scheduling cyber security training for staff upon commencement and annual refresher training for all staff and Councillors
- Sharing relevant examples of data breaches with staff, Councillors and Council's Audit, Risk & Improvement Committee (ARIC), when and where appropriate.

Council will require all contracts with contractors / third party providers who may have access to, be provided with, or hold Council Held Information, to contain obligations requiring the contractor to:

- Report data breaches of their products and / or systems to Council within certain timeframes of a data breach being identified
- Take mitigating actions to prevent data breaches and take similar mitigating actions to prevent further impacts following the identification of a data breach
- Provide assistance to Council in undertaking assessments of any identified data breach
- Identify how they will notify any affected individuals (with the concurrence of Council) and provide support to affected individuals in the event of a data breach
- Adhere to Council's Privacy Management Plan when handling any private or confidential information, including personal or health information.
- Adhere to all Council policies, including this Data Breach Policy.

For data breaches that involve other public agencies, the General Manager (or delegate) will directly liaise with the other affected agencies in respect of any notification requirements for the MNDB.

It should be noted that Council will only ever publish high-level information about the specific controls that are in place, in an effort to reduce any further risks.

10 Tax File Numbers (TFN)

Although NSW public sector agencies are exempt from most of the federal Privacy Act 1988 (Cth), the data breach notification requirements in relation to TFN's do apply.

All organisations which receive TFN's, whether from new employees or in other circumstances, must comply with the Privacy (Tax File Number) Rule 2015 (the TFN Rule). The TFN Rule is issued under section 17 of the federal Privacy Act, and sets out requirements for the collection, use, disclosure, data security and disposal of individuals' TFN information.

A breach of the TFN Rule is considered an eligible data breach, and therefore an organisation which experiences a data breach involving TFN's must comply with the MNDB

scheme under the federal Privacy Act. This involves notification to the affected individuals, and to the Australian Privacy Commissioner.

Importantly, the internal Council reporting process for managing a breach that includes TFN's, will follow the same process as a breach that does not include TFN's, simply for ease of application, noting that the Assessor and other relevant staff will manage the formal notification process of a TFN breach.

11 Responding to a data breach

The quicker Council can detect a data breach, the better the chance that it may be contained and potential harms mitigated through prompt action.

Who to contact if you suspect a data breach?

Your immediate contact should be:

Jennifer Chenhall
Manager Governance & Risk (Privacy Officer / Assessor)

Email: jennifer.chenhall@woollahra.nsw.gov.au
Phone: **02 9391 7012**
Mobile: [redacted]

You must then inform your **Manager** and your **Director**

As noted above, in all cases, Council Officers must report a suspected data breach immediately, either in person or by phone call, to the Privacy Officer (Assessor), their Manager and Director. Report in person or by phone and then confirm your report in writing, by email.

If the Privacy Officer believes the suspected data breach is likely to result in serious harm to any individual, they must report it immediately to the General Manager, with the General Manager to decide whether to constitute or activate the Data Breach Response Team (DBRT).

Data breaches will be dealt with on a case-by-case basis by undertaking an assessment of the data breach and the specific risks involved and by undertaking a risk assessment to decide the appropriate course of action. It should be noted that every response will need to be considered holistically and will be dependent on the nature, severity and impact of any data breach and noting that data security methods must be commensurate with the sensitivity of the information the subject of the data breach.

It should be noted that if the data breach is the result of Council staff behaviour or actions, then any disciplinary action taken will also be commensurate with the seriousness of the breach.

There are five key steps to consider in the process of responding to a data breach, which include:

1. Report
2. Contain

3. Assess and React
4. Notify (relevant authorities and affected individuals)
5. Review

Steps 1 - 3 will be followed for all data breaches, with Steps 4 & 5 only needing to be followed if the preceding steps result in any notification requirements or review requirements, including for any data breaches that include TFN's. Each step will be considered and implemented to the appropriate extent in responding to a data breach.

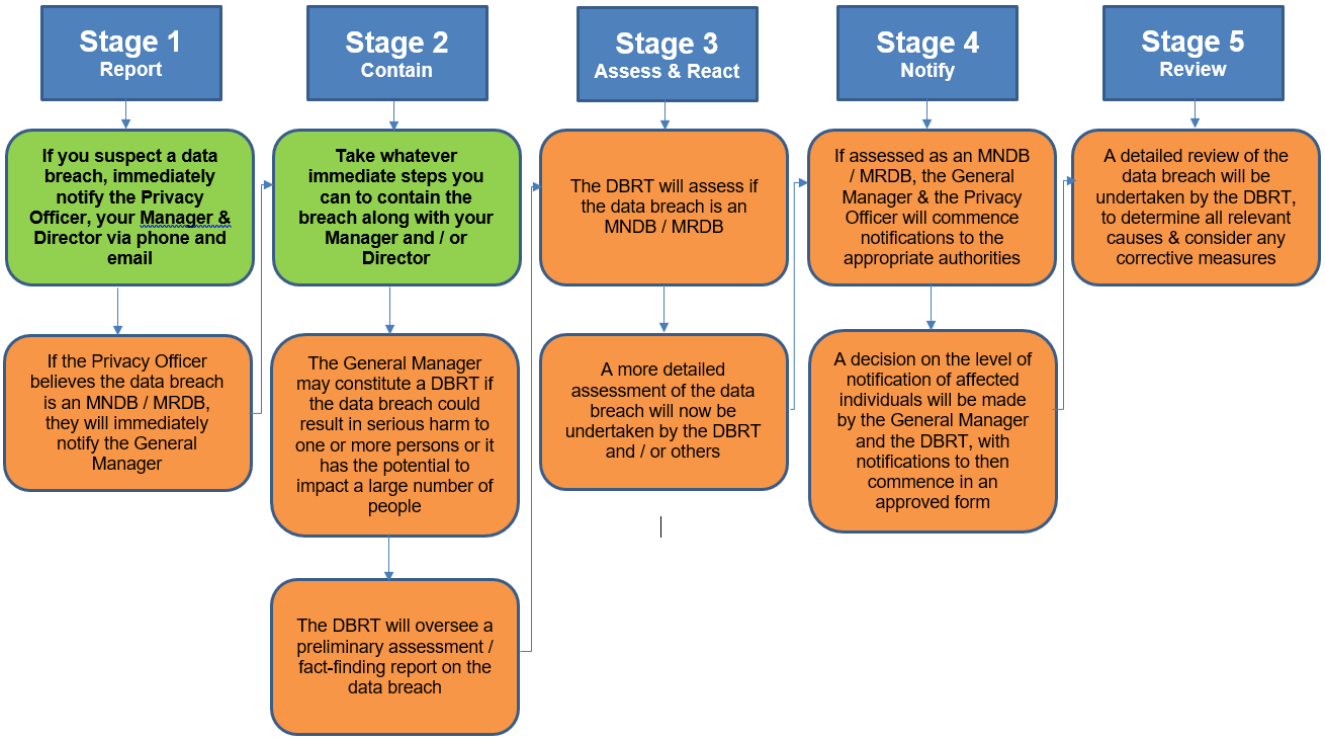
The following flow chart provides a high level overview of the process to follow when responding to a data breach. More detailed information on the response process can be found at **Attachment A.**

Please note that as detailed in Section 10, a breach of the TFN Rule is considered an eligible data breach, and therefore Council must comply with the MNDB scheme under the federal Privacy Act. This involves notification to the affected individuals, and to the Australian Privacy Commissioner.

Importantly, for any staff who suspect a data breach that involves TFN's, the internal Council reporting process for managing a TFN breach will follow the same process as a breach that does not include TFN's as detailed in the flowchart below and in **Attachment A**. It should be noted that the Assessor and other relevant staff will manage the formal notification process of a TFN breach.

For information, **Attachment B** includes a list of matters to be considered when the Privacy Officer undertakes Steps 2 & 3 when responding to a data breach, noting that this list is not exhaustive.

FOR ALL STAFF: Please note that the two boxes shown in **bold** below in the flowchart (i.e. the first boxes in Stage 1 & Stage 2), tell you what you need to do in the case of a suspected data breach:



12 Processes for responding to incidents that involve another entity

The relevant contact officer (for a third party entity / Contractor) within Council will provide the Privacy Officer with appropriate contact details, so that they can make contact with the third party as required, in order to commence gathering the information required to assist in assessing the breach and conducting any required risk assessment etc

13 Communications Strategy

The MCE will be responsible for all communications (internal and external) issued under this Policy, with the concurrence and approval of the General Manager, noting that the General Manager (or delegate) is the key spokesperson.

Council will aim to notify affected individuals and external reporting agencies as soon as practicable, once a data breach and or an incident of unauthorised access has been confirmed as having occurred, in line with the processes detailed throughout this Policy.

Any information included in a notification will have regard for this Policy as well as Council's Privacy Management Plan. Where engagement with external reporting authorities is required, the MCE will liaise and consult with the Assessor and the General Manager as required. A sample notification is included at **Attachment D**, noting that each notification may be different, dependent on the type and scope of the data breach being notified.

If Council's Business Continuity Plan is activated, then the communication requirements for that Plan are to be managed in conjunction with the communication requirements included in this Policy.

14 Record keeping

Appropriate records must be maintained to provide evidence of how suspected data breaches are managed, including those not escalated to the DBRT or notified to the IPC or the OAIC.

Tracking data breaches will allow Council to monitor, analyse and review the type and severity of suspected data breaches, along with the effectiveness of the response methods. This may help to identify key recommended actions for improvement that may assist in remedying weaknesses in security or processes into the future.

Council will meet its record keeping obligations under the PPIP Act by:

- Maintaining and publishing (on our website) a Public Notification Register for any notifications given under section 59N(2) – see example at **Attachment C**.
- Establishing and maintaining an internal register for Eligible Data Breaches
- Publishing our Privacy Management Plan and this Policy on our website.

15 Community Strategic Plan, Delivery Program and Operational Plan

This Policy relates to Themes, Goals and Strategies outlined in Council's Community Strategic Plan Woollahra 2032 and Priorities outlined in Council's Delivery Program and Operational Plan, specifically:

Theme:	Civic Leadership	
Goal:	A well-managed Council	
Strategy:	11.3	Ensure effective and efficient governance and risk management.
Priority:	11.3.2	Ensure corporate risks are managed appropriately to reduce the likelihood of any adverse impacts to Council or the community.

16 Relevant legislation

- Privacy and Personal Information Protection Act 1998 (PPIP Act)
- Privacy Act 1988 (Office of the Australian Information Commissioner)
- NSW State Records Act 1998
- Government Information (Public Access) Act 2009
- Health Records and Information Privacy Act 2002

17 Policy review & amendment

In general, Council policies are reviewed every two years or in accordance with legislative requirements. The IPC Guide to Preparing a Data Breach Policy (May 2023) states that as both the external threat environment and agencies' internal makeup and functions are continuously developing and changing, this policy should be regularly reviewed to ensure it remains fit for purpose.

In following this guidance, this Policy will be reviewed annually and updated accordingly and testing of the processes included in the Policy will be undertaken as a component of Council's Business Continuity Plan testing.
Any amendments to this Policy must be by way of approval of the General Manager.

Related Policies and Procedures

	HPECM Reference
Privacy Management Plan	17/183435
Business Continuity Plan Framework (Draft)	24/37678
Business Continuity Policy (Draft)	24/37677

Policy Amendments

Date	Responsible Officer	Description
01/03/2024	General Manager	Final draft of policy and adoption of the document

ATTACHMENT A

Responding to a Data Breach – Detailed Steps

There are five key steps to consider in the process of responding to a data breach, which include:

1. Report
2. Contain
3. Assess and React
4. Notify relevant authorities and affected individuals
5. Review.

Steps 1 - 3 will be followed for all data breaches, with Steps 4 & 5 only needing to be followed if the preceding steps result in any notification requirements or review requirements. Each step will be considered and to the extent appropriate, implemented in responding to a data breach.

Step One: REPORT

- Any Council Officer who becomes aware of a data breach or suspects a data breach, will immediately notify the Privacy Officer and their relevant Manager and Director. Refer to Clause 6 for the definition of what a data breach is.

- Where the Privacy Officer has reasonable grounds to believe that the data breach is an MNDB / MRDB, then they will notify the General Manager (or delegate) immediately.

- When reporting a possible MNDB / MRDB to the General Manager (or delegate), the Privacy Officer will also indicate whether in their opinion it is likely to take more than 30 days to determine if the data breach is an MRDB (if known), based on the evidence before them at this stage in the process.

- The Privacy Officer, on being notified of a data breach will call and notify the Council's insurer and Council's legal advisors.

Step Two: CONTAIN

- All Council Officers (where possible), in conjunction with their relevant Manager and/or Director, will take all immediate steps to contain any data breach to the best of their ability, by limiting the extent and duration of the unauthorised access to or disclosure of Council Held Information, and preventing the data breach from intensifying.

- The above obligation is ongoing as other steps proceed.

- A Data Breach Response Team (DBRT) will be constituted if it has been determined by the General Manager and the Privacy Officer that the data breach could result in serious harm to one of more persons, or the data breach is of such a nature that it has the potential to affect a large number of people and the notification provisions of this policy are triggered, or it is deemed to be an eligible data breach.

- The DBRT will include as a minimum the General Manager, Director Corporate Performance (DCP), Manager Governance & Risk (MG&R), Manager Information & Digital Transformation (MI&DT) and the Manager Communications & Engagement (MC&E) and the Manager / Director of the area where the data breach has occurred. If a third party provider or other agency is involved in the data breach, then there may be grounds to constitute a Joint Response Team, which is a decision that rests with the General Manager.

- The DBRT will oversee preliminary fact-finding about the data breach including the type of data (i.e. check if TFN's were involved), cause, risk of spread of the data breach and options to mitigate.

- The DBRT will make a preliminary assessment of the risk posed by the data breach as Low, Medium or High according to the risk criteria below. This decision is to be documented in an agreed report template.

Please note that any breach that includes TFN's will immediately be considered High risk.

Risk Assessment	
Low risk data breach means:	A loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur (e.g. paper files are left behind in a meeting but are later retrieved).
Medium risk data breach means:	A loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent and that the data is somewhat protected (e.g. a laptop with encrypted data is left on a bus).
High risk data breach means:	It is reasonably believed that the data breach is ***likely to result in serious harm*** to one or more of the individuals to whom the information relates (e.g. external hackers / threat actor breaches our firewall & obtains valuable customer data). Any data breach that includes TFN's.

The level of risk assigned to a data breach will determine who else needs to be informed about the data breach, with consideration to be given to both internal and external stakeholders.

Step Three: ASSESS and REACT

Assessment of the data breach

- If it is suspected that an eligible data breach has occurred, the General Manager (or delegate) along with the Director Corporate Performance, the Manager Governance & Risk and the Manager Information & Digital Transformation will assess whether an eligible data breach has actually occurred. This is known as an Eligible Data Breach Assessment. The General Manager (or delegate) may constitute the DBRT to assist in this regard.

- After completing an Eligible Data Breach Assessment, the General Manager (or delegate) will make a final decision on whether the data breach is (or there are reasonable grounds to believe the data breach is) an Eligible Data Breach.

- The General Manager (or delegate), along with the Privacy Officer will also assess and consider whether a data breach is a Commonwealth Notifiable Data Breach. Commonwealth Notifiable Data Breaches are specific to unauthorised access or disclosure of TFNs. Council has 30 days to complete this assessment from the date of the initial report of the data breach.

General Assessment

- Under this step in the process, Council will conduct a more detailed assessment than the earlier preliminary assessment of a data breach by gathering all relevant information in respect of the data breach.

- For all data breaches, Council will evaluate the risks associated with each breach, with the following factors to be considered:
    - What Council Held Information has been lost or disclosed?
    - What is the nature of the Council Held Information that has been lost or disclosed?
    - What was the cause of the data breach?
    - Who is affected by the data breach?
    - What combination of information was lost? Certain combinations or types of Personal Information can lead to increased risk.
    - How long the information has been accessible? The length of time of unauthorised access to, or unauthorised disclosure will increase risks of harms to individuals.
    - How many individuals were involved? The scale of the data breach will likely affect the Council's assessment of likely risks.
    - If the data breach involves TFN information?
    - Was it a one-off incident or does it expose a more systemic vulnerability?
    - What steps have been taken to contain the data breach? Has the Council Held Information been recovered? Is the Council Held Information encrypted or otherwise not readily accessible?
    - What is the foreseeable harm to affected individuals/organisations?
    - Who is in receipt of the Council Held Information (if known)?
    - What is the risk of further access, use or disclosure, including via media or online?
    - Are other public agencies involved in the data breach?

React

- Where a third party has gained possession of Council Held Information and declines to return it (if indeed the Threat Actor has been identified), the General Manager (or delegate) will engage external legal advice on what action can be taken to recover the Council Held Information.

- When recovering Council Held Information, the Council will endeavour to ensure that copies of the Council Held Information have not been made by a third party or, if they have, that all copies are recovered.

- Council will ensure that all actions to manage, contain, mitigate and remediate the impact of a data breach in order to prevent future data breaches are considered and implemented.

Step Four: NOTIFY

Eligible Data Breach Notification

The General Manager (or delegate) will notify the Information & Privacy Commissioner (IPC) immediately after determining that a data breach is an Eligible Data Breach.

Notification to the IPC will be made in the approved form by the Privacy Commissioner as published on the IPC's website.

The General Manager (or delegate) and DBRT (if constituted) will determine how to notify and oversee the notification to Affected Individuals of the Eligible Data Breach in accordance with this Policy and any formal guidance provided by third party agencies, Council's insurers and / or legal advisors, noting that the notification process may be undertaken by a third party on behalf of Council.

Commonwealth Notifiable Data Breach Notification

The General Manager (or delegate) and the Privacy Officer will notify the OAIC and any affected individuals as soon as practicable after identifying a Commonwealth Notifiable Data Breach.

The General Manager (or delegate), the Privacy Officer and the DBRT (if constituted) will determine how to notify and oversee the notification made to the OAIC and any affected individuals of the Commonwealth Notifiable Data Breach.

Voluntary Data Breach Notification for Non-Eligible Data Breaches

As a matter of best practice, Council will also consider voluntary data breach notification to the IPC, affected individuals and others, if the data breach is a Non-Eligible Data Breach. This will be at discretion of the General Manager.

Notification of individuals affected by a Mandatory Reporting Data Breach (MRDB)

Council will notify affected individuals either directly or via a third party provider (i.e. ID Support NSW), by telephone, letter, email or in person.

Indirect notification may take place, such as information posted on the Council's website, a public notice in a newspaper, or a media release. This will generally occur where the contact information of individuals who are affected are unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop or iPad as to the value of the information contained).

Council will maintain a public notification register in accordance with s59N(2) and s59P of the PPIP Act. This register will be published on Council's website.

Council will also maintain an internal Data Breach Incident Register, which will include the following information (where practicable), for all Eligible Data breaches:

- Date of the breach
- Description of the breach
- Who was notified of the breach?
- When was the breach notified?

- The type of breach (e.g. unauthorised access, unauthorised disclosure, loss of information)
- Details of the steps taken by the Council to contain and mitigate harm done by the breach
- Details of the actions taken to prevent future breaches
- The estimated cost of the breach etc.

All Notifications

Council will at all times and for every data breach, consider other internal and external notifications and approvals and communicate with such external agencies and stakeholders as is reasonably required in the individual circumstances of a particular data breach e.g. the Police, NSW Department of Customer Service (ID Support NSW), Cyber Security NSW, the Australian Tax Office, the OAIC etc.

Step Five: REVIEW

Understanding what went wrong, how issues were addressed and whether changes are needed to processes and procedures following a data breach will mitigate future risks and are key to ensuring Council continues to proactively manage data breaches in line with legislation and general community expectations. The following steps will be undertaken:

- Council will conduct a detailed review of all data breaches to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

- From its review of a particular data breach, Council will undertake any recommended steps to further mitigate and remediate Council's procedures, policies and IT systems to prevent future data breaches.

- A post-incident review will consider:
    - A cause analysis of the data breach
    - Security audit of both physical, technical and cyber security controls;
    - Review of employee training practices;
    - Review of contractual obligations with contracted service providers;
    - Any other review considerations, recommendations or guidelines published by the IPC and or other agencies.

A confidential report of all high risk data breaches, all Mandatory Reporting Data Breaches and all Commonwealth Notifiable data breaches will be made to Council's Audit, Risk and Improvement Committee and to a confidential Councillor briefing, workshop or similar, noting that any information that is publicly reported will be at a high-level so as not to expose Council or the community to any greater risks.

ATTACHMENT B

Data Breach Response Report – Matters for Inclusion

Step 1 – Report	
1.1	When did the Data Breach occur (if known)?
1.2	When, how and by whom was the Data Breach first discovered?
1.3	When, how and by whom was the Data Breach first reported to the Privacy Officer?
1.4	What was the primary cause of the Data Breach (if known at this stage) i.e. malicious or criminal attack; system fault; human error
Step 2 – Contain	
2.1	What steps have been taken to contain the Data Breach?
2.2	What steps have been / should be taken to minimise the effect on potentially affected individuals?
2.3	Has a Data Breach Response Team (DBRT) been stood up and if so, who has been drafted into the DBRT (include both internal & external stakeholders and the date each role was added)
2.4	What steps have been / should be taken to prevent reoccurrence? (Consider here whether any similar breaches have occurred in the past.)
2.5	What is the DBRT's conclusion as to the level of risk posed by the data breach at this stage? (Include supporting reasons.) • High Risk • Medium Risk • Low Risk
Step 3 – Assess & React	
3.1	Outline the nature of the Data Breach as first reported to the Privacy Officer: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information • Cause of breach / how it occurred • Type of data affected: financial / government identifiers (e.g. Medicare number or passport number) / Tax File Numbers / contact information (e.g. home address, phone number or email address) / health information / Other • Type of individuals affected • Number of individuals affected (if known)
3.2	Has a third party gained possession of Council Held Information? If so, what steps have been taken to recover this?

3.3	What is the preliminary view as to the level of risk posed by the data breach? • High Risk – likely to result in serious harm to affected individual/s and or includes TFN's • High Risk – large numbers of people impacted • Medium Risk • Low Risk
3.4	Outline the results of the preliminary fact-finding: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information • Cause of breach / how it occurred • Type of data affected: financial / government identifiers (e.g. Medicare number or passport number) / Tax File Numbers / contact information (e.g. home address, phone number or email address) / health information / Other • Type of individuals affected • Location of individuals affected • Number of individuals affected
3.5	Have any external parties been notified about the breach i.e. insurers, legal advisors, Police, IPC, AOIC, Cyber Security NSW (Include date and details)
Step 4 – Notify	
4.1	Decision taken in relation to notification? (Include supporting reasons and date/s decision made and by whom.) • Mandatory (all High Risk breaches) • Voluntary (optional for all other Medium Risk breaches) • No notification (Low Risk breaches)
4.2	What pre-notification steps have concluded? For example, establish telephone hotline (Council or 3rd party), a dedicated webpage or web banner, social media posts, Mayoral column, print & online media. (Include date completed and details.)
4.3	Relevant formal notifications made to the IPC and / or (OAIC) Include date notification / statement made and how it was lodged. (Attach a copy to this report.), including is this Data Breach is a Commonwealth Notifiable Data Breach.
4.4	What notification method/s have been followed for notifying affected individuals? i.e. direct to only individual/s at risk of serious harm; direct to all individuals whose data was breached; indirect via our website (mandatory if neither of the above is possible); indirect via other channels e.g. social media.
4.5	Has notification been made to affected individual/s? (Include date notification made, how many people communicated with, how notification was made). (Attach a copy of the notification/s to this report.)
4.6	Has the public notification register been updated in relation to this Data Breach? If so, when i.e. date and description.

Step 5 – Review	
5.1	What has been done to prevent a recurrence of this Data Breach?
5.2	Undertake a review of the organisational response, including mitigation strategies in place i.e. information security protocols; physical security controls; policies, plans or procedures; staff training; other.
5.3	Recommended plan to review / audit processes to ensure that any corrective actions are implemented.

ATTACHMENT C
Register of Public Data Breach Notifications - Example Only

Register of Public Data Breach Notifications

Privacy and Personal Information Protection Amendment Act 2022 - Section 59N(2)

Council may choose not to include information in this Register where the principles of Section 59P(3)(b) apply.

This register includes details of public notifications of eligible data breaches required under the Privacy and Personal Information Act 1998 (PPIP Act).

A public notification is provided when it is not reasonably practicable to notify any or all of the individuals affected by the breach directly. Woollahra Municipal Council will retain notifications in this register for a period of 12 months.

Council Data Breach Identifier #	Date of data breach	Date Council became aware of data breach	Description of data breach	How the breach occurred	Type of personal information impacted (e.g address, bank information, superannuation details, TFNs etc)	Actions taken or planned to mitigate harm to individuals	Recommended steps individuals should take to further protect their data	Date public notification was published	Name of Contact Officer for assistance	Link to full public notification details on Council's website
N/A - There have been no notifications made in the previous 12 months										

ATTACHMENT D

Example of a Customer Notification

To: [redacted] by email: [redacted]

[redacted]

Reference number: [redacted]

Notification of a potential data breach - customers of Woollahra Libraries

Dear [redacted]

I'm writing to inform you of a recent cyberattack on a third-party software system that Woollahra Council Libraries uses to manage a range of activities such as computer access, room bookings, printing and scanning, and payment of library fines. While our investigation into this matter is ongoing, we wanted to notify you promptly about the possible access to your personal information and provide you with precautionary steps and support to protect your information.

What information was affected?

The type of information stored in the software is limited to contact details of customers who have used one of the above-mentioned services at one of our Libraries. The information stored could include your name, email address, mobile number, landline number and postal address.

For a small number of customers, the system also stored encrypted passwords used to access the booking system and some also contained partial credit card payment details.

How you may have been affected?

While we have not been able to confirm that information has in fact been stolen or breached as a result of this cyber-attack, it is possible that some of your personal information may have been accessed. The system impacted by this potential data breach contained the following personal information relevant to you:

- Email address
- Family (surname/last) name
- First (given) name
- Mailing address
- Mailing address
- Mobile number

Actions taken by Woollahra Council:

As soon as we detected this cyber-attack on [redacted], we isolated the affected system to prevent further unauthorised access to it. We also notified the Australian

Cyber Security Centre and Cyber Security NSW and we engaged a specialist cyber forensic firm to investigate the potential data breach. In addition to this, the provider of the software that was breached, has developed a software fix to the address the vulnerability in their system.

To be clear, the investigation to date has determined that the unauthorised access was limited to the third-party software in use by our Libraries and has not impacted other Woollahra Council systems.

Whilst we are still investigating this potential data breach, we wanted to inform you of the risk that some of your personal data may have been breached in this cyber-attack as soon as possible and to provide you with advice on what actions to take.

We take our role as the custodians of customer information seriously and do all we can to ensure the privacy and protection of personal data, which is why we have taken the actions we have to date. At the outset, we sincerely apologise for any distress this potential data breach may cause.

Actions you can take:

When your personal details are involved in a data breach, it's important to stay alert for scams that may come to you by phone, post, or email. Some scams look like they come from trusted or well-known sources. You can take action and protect yourself from the risks following a data breach by:

- verifying all communications you receive to ensure they are authentic.
- avoiding texts or emails from numbers or email addresses that you do not recognise or find suspicious.
- keeping an eye on your bank accounts for any strange or fraudulent activity.
- change your passwords regularly, and make sure they are long and strong.

We are using the services of ID Support NSW, which is a service provided by the NSW Government that helps customers if their personal information or identity credentials are stolen or fraudulently obtained.

If you are concerned that your personal information may have been breached, please contact **ID Support NSW**, **Monday to Friday between 9am and 5pm** on **1800 001 040** (interpreter services available) or visit the website at https://www.nsw.gov.au/id-support-nsw.

ID Support NSW provides guidance on how to restore and protect the security of your identity. When you call, you will need your unique reference number, being 00042015.

We understand that just the thought of having your personal information compromised can be distressing, so if you require support, please contact the 24/7 Mental Health line on 1800 011 511.

Yours sincerely

Craig Swift-McNair
General Manager, Woollahra Council

Complaints
If you are not satisfied with the response in relation to this potential data breach, you can email us at records@woollahra.nsw.gov.au to request an internal review. You may also make a complaint directly to the NSW Privacy Commissioner. Further information on your review rights is available from the Information and Privacy Commission NSW (IPC) at https://www.ipc.nsw.gov.au/privacy/citizens/make-complaint.

How can you confirm this message is real?
We know how important it is to check correspondence for authenticity. For your security and trust, we have not requested you provide personal information. This notification has been provided so you have control and support options to protect your personal information. You can check that ID Support is a real Government service by searching ID Support NSW from your browser or type the following into your web address window https://www.nsw.gov.au/id-support-nsw.

Privacy collection
If you contact ID Support NSW about this letter, the customer support team may ask for more information to better assist you. The Privacy Statement of ID Support NSW details the personal information that is collected and the way it is managed. ID Support NSW adheres to the regulations outlined in the Privacy and Personal Information Protection Act of 1998 and the Health Records and Information Privacy Act of 2002. ID Support's privacy statement is available on the NSW Government website (nsw.gov.au).

ATTACHMENT E

Data Breach Notification to the NSW Privacy Commissioner

(For use by the Privacy Officer / General Manager)

information and privacy commission new south wales

Mandatory Data Breach Reporting Form

[redacted]

Data Breach Notification to the Privacy Commissioner

Section 59M of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires the head of a public sector agency to immediately notify the Privacy Commissioner of an eligible data breach using an approved form. This form has been approved by the Privacy Commissioner for use by agencies for the purpose of notification under section 59M of the PPIP Act.

This approved form sets out the information that agencies must supply to the Privacy Commissioner when making a notification of an eligible data breach, unless it is not reasonably practicable to provide that information.

This document is not to be used for agency's notification to individuals affected by a breach, however the information supplied may be of use when developing your agency's written notification as required by section 59N of the PPIP Act.

Agency making notification

Agency name:

Agency address:

Telephone number:

Contact name:

Contact telephone:

Contact email:

Contact role/title in organisation:

Notification made on behalf of another agency/agencies (if applicable)

Is the notification made on behalf of another agency/agencies? Yes ☐ No ☐

If yes, complete the agency details below:

Name:

Address:

Telephone number:

Contact name:

Contact telephone:

Contact role/title in organisation:

If the notification is made on behalf of more than one agency, please provide the above details for each agency as a separate attachment.

Data Breach Notification Form

Type of personal information that was the subject of the breach

Select the option(s) that best apply:

☐ Contact details

☐ Identity documents/credentials

☐ Financial information

☐ Health information

☐ Under review (agency is still conducting its assessment at time of notification)

☐ Other sensitive information:

Description of eligible data breach

Discovery of the breach

When the data breach occurred:

When the data breach was discovered:

Where the data breach was discovered:

How the data breach was discovered:

By whom was the data breach discovered:

Amount of time the personal information was exposed:

Type of breach

Select the **type(s) of data breach** as applicable:

☐ Unauthorised disclosure

☐ Unauthorised access

☐ Loss of information

☐ Other:

How the breach occurred

Provide a brief explanation as to how the breach occurred:

Cause of breach

☐ Cyber Incident

If the breach was caused by a Cyber Incident, select the type of Cyber Incident below:

Data Breach Notification **Form**

- ☐ Ransomware
- ☐ Malware
- ☐ Phishing (compromised credentials)
- ☐ Compromised credentials (method unknown)
- ☐ Hacking
- ☐ Brute Force Attack (compromised credential)
- ☐ Other:

☐ Human Error

☐ Loss/theft of data/equipment

☐ System fault

☐ Other:

Remedial action taken to date (including description of action and when)

Remedial action to be taken

Notification to affected persons

Total number of individuals affected, or likely to be affected by the breach (provide best estimate if exact figure is unknown):

Total number of individuals notified of the breach at this stage:

Total number of individuals yet to be notified of the breach:

Provide details of how and when individuals were notified:

Have individuals been advised of the complaints and internal review procedures under the PPIP Act?

Recommendations made to affected individuals about the steps they should take to mitigate the effects of the breach

Estimated cost

Estimated cost of the breach to the agency:

Other bodies notified

Data Breach Notification **Form**

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au