INNER WEST

Data Breach Policy

V1

IWC1202/0922

Title	**Data Breach Policy**
Summary	The Policy outlines Council's strategy for managing data breaches in line with Council's commitment to protect Personal Information in accordance with the *Privacy and Personal Information Protection Act 1998* and particularly the Mandatory Notification of Data Breach scheme implemented under that statute (per the amendments introduced by the *Privacy and Personal Information Protection Amendment Act 2022*).
Document Type	Policy
Relevant Strategic Plan Objective	Strategic Direction 5: Progressive responsive and effective civic leadership.
Legislative Reference	• *Local Government Act 1993* • *Government Information (Public Access) Act 2009* • Government Information (Public Access) Regulation 2018 • *State Records Act 1998* • *Privacy and Personal Information Protection Act 1998* • *Privacy and Personal Information Protection Amendment Act 2022* • *Health Records and Information Privacy Act 2002* • *Privacy Act 1988 (Cth)*
Related Council Documents	• Model Code of Conduct • Privacy Management Plan • Data Breach Policy • Data Breach Procedure • Risk Management Policy • Risk Management Procedure
Version Control	See last page

INNER WEST

Contents

1 Purpose

The purpose of this policy is to provide guidance to Council Officials in responding to a Data Breach, whether it is deemed to be a minor Data Breach, or a Data Breach that is notifiable under the New South Wales Mandatory Notification of Data Breach (**MNDB**) scheme established under Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW). The purpose of this policy is also to provide guidance to Council Officials, service providers/service partners, volunteers and members of the public on how to report actual or suspected Data Breaches and the process that Council will take to respond to such Data Breaches.

For the purposes of this policy, a Data Breach will include the unauthorised access, unauthorised disclosure or loss of Personal Information, Health Information and Commercial Information.

2 Scope

This policy applies to all Council Officials, service providers/service partners, volunteers and members of the public.

3 Definitions

In the Data Breach Policy, the following terms have the following meanings:

Act	*Local Government Act 1993.*
Commercial Information	Any commercial information, whether it be that of Council's, external stakeholder's or provided by a service provider/service partner in confidence. Note that commercial information does not fall within the MNDB scheme unless it contains Personal Information or Health Information.
Confidential Information	Information and data including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of residential buildings, Security Classified Information and information related to Council's IT/cyber security systems.
Councillor	Inner West Council elected representative.
Council committee member	A person other than a Councillor or Council Officer who is a member of a Council committee other than a wholly advisory

	committee, and a person other than a Councillor who is a member of Council's Audit, Risk and Improvement Committee.
Council Officer	Inner West Council members of staff (including full-time, part-time, casual and contracted staff).
Council Official	Councillors, Council Officers, Council committee members and delegates of Council.
Data Breach	An incident where an unauthorised access to, or unauthorised disclosure or loss of, Personal Information or Commercial Information held by Council has occurred. Data Breaches can occur between local governments, within Council or external to Council (such as by a service provider/service partner).
delegate of Council	A person (other than a Councillor or Council Officer) or body, and the individual members of that body, to whom a function of Council is delegated.
Eligible Data Breach	A Data Breach that would be likely to result in serious harm to an individual to whom the information that is the subject of the Data Breach relates.
Health Information	Information or an opinion about a person's physical or mental health or disability, or information relating to the provision of health services to a person. Health information can include a psychological report, blood tests or an x-ray, results from drug and alcohol tests, information about a person's medical appointments, and information regarding vaccination status. It can also include some personal information that is collected to provide a health service, such as a name and telephone number. For the purposes of the MNDB scheme, Health Information is Personal Information.
MNDB scheme	Mandatory Notification of Data Breach scheme in New South Wales.
Personal Information	Information or an opinion about a person where that person's identity is apparent or can reasonably be ascertained. This information can be in a database and does not necessarily have to be recorded in a material form. For the purposes of the MNDB scheme, Personal Information includes Health Information.

Privacy Contact Officer	The Council Officer responsible for receiving reports of Data Breaches and administered the requirements set out in this Data Breach Policy and the Data Breach Procedure. Council's Right to Information Officer serves as Council's Privacy Contact Officer.
Response Team	The team that will assemble in the event of a Data Breach, and includes, at minimum, the following personnel: • Right to Information Coordinator (Privacy Officer) • Senior Manager Governance and Risk • Risk and Audit Manager • Governance Manager • Chief Technology Officer • ICT Infrastructure Manager • IT Business Solutions Manager • IT Support Manager • The custodian of the data effected by the Data Breach. The Response Team may be expanded depending on the seriousness of the Data Breach, particularly if the Data Breach is deemed to be an Eligible Data Breach, in accordance with the Data Breach Procedure.
service provider/service partner	A person or company engaged to provide services to Council.
unauthorised access	When an internal or external individual or an organisation gains access to the information of an organisation or individual without permission. Examples include a Council Officer browsing Council records for identity information of residents without a legitimate purpose or an online database being compromised by hackers resulting in financial details of individuals being accessed.
unauthorised disclosure	The deliberate or inadvertent making of the information of individuals or organisations available or accessible to unauthorised parties by Council Officers without the authority to do so. Examples include the disclosure of Personal Information by a Council Officer whilst discussing their work and duties with friends and family external to Council or online via social media.

volunteer	A formally recognised, unpaid member of the public who helps provide Council services e.g. Visitor Information Centre/Library.

4 Statement

Council is committed to protecting any Personal Information held, including that of its own Council Officials, volunteers, service providers/service partners and community members. To ensure such protection, Council has strict obligations for the management of Personal Information, which is set out in Council's Privacy Policy and Privacy Management Plan. While every measure is taken to protect Personal Information, Council acknowledges the significant risks of Data Breaches, particularly with growing technological advancement and the increased rate of cyber-attacks. In preparedness for such Data Breaches, Council has prepared this Data Breach Policy to demonstrate how Council will respond to reduce the impacts of a Data Breach in the event that one should occur.

This Data Breach Policy addresses the processes that will be taken in the event that there is an Eligible Data Breach, which is required to be notified to the NSW Privacy Commissioner pursuant to the *Privacy and Personal Information Protection Act 1998* (NSW).

5 Measures taken to prepare for Data Breaches

Training and awareness

Council disseminates information about its procedures for Data Breaches to Council Officials along with the Privacy Management Policy and Privacy Management Plan.

Council will:

- Ensure that Council Officers receive a copy of the Data Breach Policy when they commence employment at Council.
- Ensure that Council Officers are promptly notified of updates to the Data Breach Policy.
- Provide training and targeted advice to Council Officers and business units to help them understand how to implement the information contained in this Data Breach Policy and the Data Breach Protocol. This training will emphasise the containment, assessment and notification of Data Breaches in compliance with legislation.
- Encourage Council Officers to refer to this Data Breach Policy and the Data Breach Procedure, and to liaise with the Privacy Officer if they are unsure about a Data Breach issue.
- Ensure that Council Officers can easily access a copy of this Data Breach Policy and the Data Breach Procedure via the intranet.
- Promote awareness and compliance with Data Breach requirements by participating in promotional activities as part of the annual Privacy Awareness Week.

- Give service providers/service partners a copy of this Data Breach Policy and training where necessary depending on the extent of their involvement with Personal Information.
- Ensure that elected Council Officials and the Audit, Risk and Improvement Committee is given a copy of this Data Breach Policy and the Data Breach Procedure.

Processes for identifying and reporting breaches

Data Breaches are most commonly identified by reports from Council Officials, volunteers, service providers/service partners, members of the public or other organisations who have become aware of unauthorised Access, unauthorised Disclosure or loss of Personal Information or Commercial Information.

Please refer to section 6 of this Data Breach Policy for information on what constitutes a Data Breach. Data Breaches may also be identified by a cyber security incident such as malware, a hacking attack, ransomware, denial of services, phishing attack or a combination of these.

Council has in place several systems for the identification of Data Breaches, including comprehensive cyber security, security systems and auditing requirements which are undertaken in accordance with Council's Risk Management Policy and Procedure.

All reports of suspected or actual Data Breaches must be made to the Privacy Officer via email at Privacy@innerwest.nsw.gov.au or phone +61 2 9392 5350.

Managing collaborations and implementing contractual controls

Service providers/service partners will be provided with a copy of this Data Breach Policy where necessary. Key contacts of service providers/service partners will be kept up to date to ensure that Council's response to a Data Breach can be managed efficiently and effectively with a view to reducing the harm caused.

Any contracts entered into with service providers/service partners will include provisions which require service providers/service partners to report any Data Breaches to the Privacy Officer immediately.

Schedule for regular testing and updating of this Policy

This Data Breach Policy and the Data Breach Procedure will be reviewed annually with the Privacy Policy and Privacy Management Plan. Randomised testing will occur regularly to assess the effectiveness of Council's response to Data Breaches, and to assess whether there are any risks which need to be addressed.

6 What constitutes a Data Breach

A Data Breach is an incident where an unauthorised access to, or unauthorised disclosure or loss of, Personal Information, Health Information or Commercial Information has occurred. The information may have been compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen, or used by unauthorised individuals, whether accidentally or intentionally.

Examples of a Data Breach include:

- A database that contains individuals' Personal Information has been accessed by an unauthorised person.
- Personal information held by Council is disclosed by an unauthorised person.
- A device containing Personal Information or Commercial Information is lost or stolen.
- A cyber-attack has occurred which has resulted in stolen Personal Information.

7 Data Breach Response Strategy

Following the report of a Data Breach, the Privacy Officer and Response Team must conduct a four-step response process as expeditiously as possible.

These four steps include containing, assessing, managing, reporting, and reviewing the Data Breach.

Step 1: Containment and preliminary assessment

Council shall prioritise the containment of the Data Breach to mitigate harm. The Privacy Contact Officer will take all necessary steps possible to ensure the containment of the breach and minimisation of any resulting damage. The steps taken may involve:

- Recovering or deleting information.
- Suspending or shutting down the system that has been breached.
- Suspending or abandoning the activity that has resulted in the Data Breach.
- Changes or revoking access codes and/or passwords.

The Response Team must conduct a preliminary assessment in accordance with the Data Breach Procedure to gather facts and assess the seriousness of the Data Breach.

Step 2: Assessment, evaluation and mitigation

Assessment of actual or suspected Data Breaches will be undertaken in an expeditious manner, and in any event, within 30 days.

The Response Team will undertake the assessment in accordance with the Data Breach Procedure. Council recognises that each Data Breach is different and should be treated on a case-by-case basis. The Response Team's assessment will include, but is not limited to, the assessment of:

- The type of information affected by the Data Breach.

- Who is affected by the Data Breach.
- The cause of the Data Breach.
- The foreseeable harm to affected individuals/organisation.

Following the assessment, further mitigation strategies will be implemented as necessary in accordance with the Data Breach Procedure.

The Response Team must notify other organisations if required, such as the NSW Police Force in the case of theft, or the Australian Cybercrime Online Reporting Network in the event of a cyber attack. Further information on specific reporting requirements to other organisations, including where notification is necessary or where there is discretion, and how that discretion is exercised, is contained in the Data Breach Procedure.

Decision about the Data Breach

If the Response Team determines that the Data Breach involves the unauthorised access, unauthorised disclosure or loss of Personal Information, and that access, disclosure or loss would cause an individual serious harm, the Data Breach is an Eligible Data Breach under the MNDB scheme. Note that unauthorised access or disclosure or loss of Commercial Information is not notifiable under the MNDB scheme unless it contains Personal Information.

NOTE: A decision about whether the Data Breach is an Eligible Data Breach may be made during any of the former steps depending on its nature.

Step 3: Reporting the data breach

Reporting to the NSW Privacy Commissioner

Where it has been determined that an Eligible Data Breach has occurred, or that there is reasonable ground to believe that an Eligible Data Breach has occurred, the Council will immediately notify the NSW Privacy Commissioner. Notification requirements, including the information to be provided, is contained in the Data Breach Procedure.

Where a Data Breach is not an Eligible Data Breach, the Data Breach may still be reported to the NSW Privacy Commissioner in accordance with the Data Breach Procedure.

Reporting to the Australian Privacy Commissioner (Commonwealth Notifiable Data Breach)

The *Privacy Act 1998* (Cth) requires Council to report to the Australian Privacy Commissioner instances where a Data Breach affects the tax file number of individual/s. If this occurs, the Council will immediately notify the Australian Privacy Commissioner (c/- the Office of the Australian Information Commissioner) of the Data Breach in accordance with the Data Breach Procedure. The requirement to notify the Australian Privacy Commissioner is in addition to the requirement to notify the NSW Privacy Commissioner.

Reporting to the affected individual or organisation

The Response Team will notify each individual or organisation to whom an Eligible Data Breach relates, and provide them with information about the Eligible Data Breach in accordance with the Data Breach Procedure. Where a Data Breach is not an Eligible Data Breach, Council may still provide voluntary notification to individuals and organisations where appropriate.

Council will publish a public notification of the Data Breach if it is not reasonably practicable to inform each individual or organisation, or if the Council otherwise deems it appropriate. The public notification will be published on Council's website in accordance with the Data Breach Procedure.

After the public notification of an Eligible Data Breach is published, Council will inform the NSW Privacy Commissioner of how to access the notification.

Step 4: Reviewing the data breach

The Response Team will coordinate a further investigation into the circumstances of the breach to ensure that any processes or weaknesses in data handling that may have contributed to the Data Breach are identified and remediated. Such investigations will be undertaken in accordance with the Data Breach Procedure. This will mitigate future risks and ensure Council's proactive management of Data Breaches.

Disciplinary measures

Where a Data Breach has resulted from a deliberate act of a Council Official, Council will take disciplinary measures in accordance with the Model Code of Conduct.

Where a Data Breach has resulted from an act of a volunteer or service provider/service partner, Council may take steps to terminate their engagement.

8 Record-keeping requirements

Data Breach Register

Council will maintain an internal Data Breach Register which details:

- Who was notified of the Data Breach.
- When the Data Breach was notified.
- The type of Data Breach.
- The steps taken by Council to mitigate the harm done by the Data Breach.
- Details of the actions taken to prevent future Data Breaches.
- The estimated cost of the Data Breach.

Public notification register

Council will keep a public notification register that is available on its website. The public notification register will contain details of the Data Breaches that have been notified to the public, including all information provided to an individual or organisation when they are notified of a Data Breach. Personal Information or information that could prejudice Council's functions will not be published on the public notification register. Data Breaches published on the public notification register will remain on the register for at least 12 months.

9 Roles & Responsibilities

The following provides the key roles and responsibilities of Council Officials.

Position	Responsibilities
Council Officials, volunteers, service providers/service partners and members of the public	Required to immediately report any actual or suspected Data Breaches to the Privacy Officer.
Privacy Officer	Upon the receipt of a report of a Data Breach, the Privacy Officer will: • Immediately notify and co-ordinate the Response Team. • Complete the steps for the Data Breach response in accordance with this Data Breach Policy and the Data Breach Procedure. • If an Eligible Data Breach has occurred, follow the reporting requirements for notification of the NSW Privacy Commissioner and/or the Australian Privacy Commissioner. • Provide oversight to the Response Team, ensuring governance and compliance with register requirements. • Provide notification to affected individuals and organisations.

Response Team	Upon notification from the Privacy Contact Officer, the Response Team will:
	• Immediately assemble to review and respond to the reported Data Breach, with delineation of responsibilities undertaken depending on the nature of the Data Breach. For example, Data Breaches involving cyber-attacks will require the expertise of the:
	  - Chief Technology Officer
	  - ICT Infrastructure Manager
	  - IT Business Solutions Manager
	  - IT Support Manager
	• Follow the response requirements as set out in this Data Breach Policy and the Data Breach Procedure.
	• Consult with relevant internal and external stakeholders as required.
	• Assist the Privacy Officer with the notification requirements and register maintenance.

10 Breaches of this Policy

Breaches of this policy may result in an investigation of the alleged breach in line with relevant Council policies including the Model Code of Conduct.

Any alleged criminal offence or allegation of corrupt conduct will be referred to the relevant external agency.

11 Administrative Changes

From time-to-time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this document, such a change may be made, including branding, Council Officer titles or department changes and legislative name or title changes which are considered minor in nature and not required to be formally endorsed.

12 Version Control – Policy History

This policy will be formally reviewed annually from the date of adoption or as required.

Governance use only:

Document	**Data Breach Policy**	***Uncontrolled Copy When Printed***	
Custodian	Senior Manager Governance & Risk	Version #	Version 1
Adopted By	Council	ECM Document #	TBD
Next Review Date	TBD (Annually)		

Amended by	**Changes made**	**Date Adopted**
Governance & Risk	Policy Developed	TBD