HUNTER'S HILL COUNCIL

POLICY REGISTER

POLICY NO.	CPIMT07
POLICY TITLE	Data Breach Policy
STATUS	Council
SERVICE	Information Management and Technology
DOCUMENT ID	670978

1. PURPOSE

The purpose of the Policy is to:

- set out how Hunter's Hill Council (Council) will respond to a Data Breach in accordance with section 59ZD of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act)
- define the role and responsibilities of Council staff in relation to managing a breach
- outline the specific steps Council will follow when responding to a Data Breach
- provide a framework for quickly and effectively responding to, and managing Data Breaches
- establish how Council will keep records and maintain Council's internal and external registers of all Data Breaches
- establish Council's post-incident review process of Data Breaches

2. SCOPE

Council has adopted this Data Breach Policy (**Policy**) to inform the public of Council's procedure for identifying, responding to and the reporting of Data Breaches the subject of Council Held Personal Information.

This Policy is designed to assist the Council to meet its legal obligations in reporting Data Breaches under the PPIP Act and Privacy Act.

Part 6A of the PPIP Act establishes the NSW Mandatory Notification of Data Breach scheme (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. The MNDB scheme applies to Personal Information as defined in section 4 of the PPIP Act, and Health Information as defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act).

Council has notification obligations under the Commonwealth Notifiable Data Breach scheme, established by the Privacy Act, which requires Council to report Data Breaches (which relate to Tax File Numbers) to the OAIC.

In some cases, Council may have notification obligations to report Data Breaches to both the OAIC and the Privacy Commissioner.

Council's Privacy Management Plan provides more information on how Council may collect, use and disclose Council Held Personal Information.

3. DEFINITIONS

Council Held Personal Information	means any Personal Information and Health 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 Representative	Councillors, council staff, volunteers, delegates of the Council and members of Council committees who represent or act on behalf of Hunters Hill Council
Data Breach	means the unauthorised access to, or inadvertent disclosure, access, modification, misuse or loss of, or interference with any Council information, including Council Held Personal Information, and in this Policy and includes a potential Data Breach
DBRT	means Council's IT Governance Committee established in 2023 to support Council's Cyber Security Framework, and is Council's designated Data Breach response team for the purposes of this Policy (see section 8 of this Policy below)
Eligible Data Breach	means an 'eligible data breach' as defined in s59D of the PPIP Act
Health Information	Health information is a specific type of 'personal information' and means information defined as 'health information' under the HRIP Act
HRIP Act	means the *Health Records Information and Privacy Act 2002* (NSW)
IPC	means the Information and Privacy Commission of NSW
IT	means information technology
MNDB scheme	means the NSW Mandatory Notification of Data Breach established under Part 6A of the PPIP Act
OAIC	means the Office of the Australian Information Commissioner
Personal Information	means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual (whether living or dead) whose identity is apparent or can reasonably be ascertained from the information or opinion as set out in s4 of the PPIP Act.
PPIP Act	means the *Privacy and Personal Information Protection Act 1988* (NSW)
Privacy Act	means the *Privacy Act 1988* (Cth)
Privacy Commissioner	means the NSW Privacy Commissioner, or as otherwise defined in the PPIP Act

4. PREVENTING AND PREPARING FOR A DATA BREACH

Council have a number of controls, systems, policies and processes in place to prevent and identify actual or suspected Data Breaches.

These controls form part of Council's cyber security framework and enterprise risk management framework.

4.1 Technical preventative measures

Council have a number of technical controls and security measures in place to help prevent a Data Breach.

4.2 Monitoring

Council networks and information systems have monitoring and auditing tools in place to detect and trace any suspicious activity.

Council has an outsourced 24/7 security operations centre (SOC) that provides a managed detection and response (MDR) service.

Council conducts regular cyber security audits, penetration testing, phishing stimulation exercises and takes part in Cyber NSW and Australian Cyber Security Centre (ACSC) programs such as Cyber Hygiene Improvement Programs (CHIPs).

4.3 Training and awareness

As most Data Breaches involve a human element of some kind, building a well-trained and aware workforce is a key element of Council's defence against Data Breaches and other privacy risks.

Council is committed to creating a culture where privacy and cyber security risk management are integral elements of decision-making and where privacy, cyber security, and risk management processes are understood and consistently applied.

To do this, we will:

- enhance Council Representative's awareness of privacy and cyber principles by promoting them on Council's intranet and staff newsletter
- provide annual privacy training to all Council representatives
- share current threat trends and advice as appropriate
- provide annual cyber security training to all Council representatives
- participate in State and Commonwealth Government initiatives such as Privacy Awareness Week and Cyber Security Awareness Month
- provide annual simulation training on Responding to Data Breaches using this Policy
- develop and promote clear internal guidelines for reporting potential Data Breaches.

4.4 Contract provisions

In accordance with Council's Procurement Manual and processes, all contracts or service providers must notify Council of any alleged, suspected or actual Data Breach (regardless of whether that Data Breach is material or not). This must include incidents before, during and after the contract period.

4.5 Alignment with other policies

This Policy has been developed in accordance with Council's existing policies and procedures, including:

- Privacy Management Plan
- Cyber Security Policy
- IT Usage and Surveillance Policy
- Cyber Security Incident Response Plan
- Records Management Policy and Program
- State Records Retention and Disposal Policy
- Business Continuity Plan.

This Policy will be tested, reviewed and updated annually or in accordance with legislative changes.

The testing of this Policy will be achieved through the results obtained from Council's simulation training on Responding to Data Breaches using this Policy.

5. IDENTIFYING A DATA BREACH

5.1 Identifying a Data Breach

A Data Breach occurs when confidential, sensitive or personal information is accessed or disclosed without authorisation, or is stolen or lost.

A Data Breach can be intentional or accidental and may occur by in a range of different ways. Some examples of a potential Data Breach include:

- accidental loss of Council documents, files, or devices (mobile phone, laptop etc) that contains or holds Council information
- physical theft of Council documents, files, or devices
- personal information sent to the wrong person (for example, an email sent to the wrong person)
- Council network or system containing personal information is hacked or infected with malware
- user account is compromised (for example, through phishing or sharing of passwords)
- unauthorised disclosure of classified information (for example, positing on website or social media without consent)
- unauthorised use of, access to or modification of Council information or information systems.

Data breaches can be detected in various ways, including:

- Self-detected incidents
- Notifications from residents and the broader community
- Notifications received from service providers or vendors
- Notifications received from trusted third parties such as the ACSC and Cyber NSW

All Council Representatives and contractors should refer to Councils Cyber Security Policy and Cyber Incident Response Plan (CIRP) for more information on how to be vigilant, how to identify incidents that might occur and other types of cyber security incidents that must be reported.

Council will assess and respond to any Data Breaches reported by Council Representatives, holistically and on a case-by-case basis, depending on the nature, severity and impact of the Data Breach. Council will conduct a post-incident review of any Data Breach, and keep current an internal register of all Data Breaches which includes the assessment and review outcome of the Data Breach.

6. DEFINING AN ELIGIBLE DATA BREACH

6.1 What is an Eligible Data Breach?

An 'Eligible Data Breach' occurs where:

a) there is unauthorised access to, or unauthorised disclosure of, Council Held Personal Information or there is a loss of Council Held Personal Information in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of Council Held Personal Information; and

b) a "reasonable person" would conclude that the above would be likely to result in serious harm to one or more individuals to whom the information relates.

6.2 What is not an Eligible Data Breach?

The MNDB scheme does not apply to Data Breaches that do not involve Council Held Personal Information, or to Data Breaches that are not likely to result in serious harm to an individual.

In the event of a Data Breach that is not considered an Eligible Data Breach, Council will still assess and respond the Data Breach. Based on the findings of the assessment, Council may still provide voluntary notification to affected individuals if deemed appropriate.

Where there is doubt as to whether the Data Breach is likely to cause serious harm, Council will notify the Privacy Commissioner and affected individuals.

6.3 What is serious harm?

The term 'serious harm' is not defined in the PPIP Act. Types of harm that can arise as the result of a Data Breach are context-specific and will vary based on the circumstances and type of personal information involved in the Data Breach.

Serious harm occurs where the harm arising from the Eligible Data Breach has, or may, result in a real and substantial damaging effect to the individual. The effect on the individual must be more than irritation, annoyance or inconvenience.

Harm to an individual includes physical harm, economic, financial or material harm, emotional or psychological harm and reputational harm.

Each Data Breach must be considered on a case-by-case basis to determine if it is an Eligible Data Breach.

When assessing any Data Breach, Council must have regard to the suite of IPC guidelines as published on the IPC's website made under section 59I of the PPIP Act and as updated by the IPC from time to time.

7. MANAGING A DATA BREACH

A Data Breach can appear in various forms and degrees of severity; therefore, all Data Breaches must be assessed on a case by case basis and all assessments must be expediated.

The following steps are provided as a framework for quickly and effectively responding, with an understanding that the sequence and depth of each may need to be adjusted based on the nature of the Data Breach.

Response Step	Key Actions
1. Report and Triage	**Council Representatives** • All Council Representatives (except for Councillors) who become aware of a Data Breach or possible Data Breach must notify the Manager Digital and Customer Information and IT Business Partner. This should be carried out immediately following the incident, using the Data Breach incident form in appendix A. • All Council Representatives (except for Councillors) should also notify the Manager, Digital and Customer Information by phone or email. **Contractor / Service Provider** • Contractors or service providers who become aware of a Data Breach or possible Data Breach must report a Data Breach to their contract manager, who is responsible for reporting to the Manager Digital and Customer Information and ensuring the Data Breach incident report form is completed. **Councillors** • Councillors who become aware of a Data Breach or possible Data Breach must report the Data Breach to the General Manager, who will notify the Manager Digital and Customer Information and/or convene the DBRT. **Community** • Any residents or members of the wider community who have reason to believe a Data Breach has occurred should contact Customer Service on 02 9879 9400 or email customerservice@huntershill.nsw.gov.au. **Escalation** • Where a Council Representative and/or Manager Digital and Customer Information, believes or has reasonable grounds to believe that a Data Breach is an Eligible Data Breach, the Manager Digital and Customer Information will notify the General Manager and if appropriate, activate the DBRT to manage the response

	effort (if the incident is classified as medium or higher in accordance with CIRP or at the discretion of the General Manager).
2. Contain	• All Council Representative aware of a Data Breach must take all necessary steps to contain the Data Breach and minimise the risks and damage by limiting the extent and duration of the unauthorised access to or disclosure of Council Held Personal Information, and preventing the Data Breach from intensifying. For example, isolating affected systems, changing passwords and other security measures. • Any Council Representative that is suspected to be involved in the Data Breach may have their access suspended immediately.
3. Assess	**Assessment of Data Breaches that may be Eligible Data Breaches** • If it is suspected that an Eligible Data Breach has occurred, the Manager Digital and Customer Information will assess whether an Eligible Data Breach has actually occurred in accordance with the PPIP Act and in accordance with the suite of IPC guidelines as published on the IPC's website made under section 59I of the PPIP Act and as updated by the IPC from time to time (**Assessment**). • Council has 30 days to complete this assessment from the date of the initial report of the Data Breach. The Manager Digital and Customer Information (as delegated by the General Manager) must request an extension from the Privacy Commissioner as soon as the Manager Digital and Customer Information reasonably believes an extension of time is required to assess any particular Data Breach in accordance with section 59K of the PPIP Act. • After completing an Eligible Data Breach Assessment, the Manager Digital and Customer Information must make a final decision on whether a Data Breach is an eligible Data Breach, or there are reasonable grounds to believe that the Data Breach may be an Eligible Data Breach. • The Manager Digital and Customer Information must also assess and consider whether Council has any mandatory notification obligations under the Commonwealth Notifiable Data Breach scheme established by the Privacy Act. **General Assessment** • The Manager Digital and Customer Information must conduct a preliminary assessment of all Data Breaches by gathering all relevant information including: o the type and nature of Council Held Personal Information involved in the Data Breach o the cause(s) of the Data Breach o identity the number of affected individuals involved in the Data Breach. The scale of the Data Breach will likely affect the Council's assessment of likely risks o the combination of Council Held Personal Information involved in the Data Breach. Certain combinations of types of Personal Information can lead to increased risk o the duration and extent the Council Held Personal Information was accessible. The length of time of unauthorised access to, or unauthorised disclosure will increase risks of harm to individuals o if Tax File Number information was involved o if it was a one-off incident or whether it exposes a more systemic vulnerability in Council's systems and procedures o the steps taken to contain the Data Breach, if the Council Held Personal Information has been recovered, and whether the Council Held Personal Information is encrypted or otherwise not readily accessible o that harm caused and the foreseeable harm to affected individuals/organisations

	○ the recipient(s) of the Council Held Personal Information, the risk of further access, and the use or disclosure, including media or online access ○ if other public agencies are involved in the Data Breach. The Manager Digital and Customer Information will then (as required): ○ develop and implement a remediation action plan detailing containment, eradication and recovery activities ○ develop a communication strategy (based on the communication strategy and templates as outlined in Council's Business Continuity Plan) ○ confirm the threat has been eradicated and return affected systems/services to normal function (test systems/services to confirm expected functionality).
4. Notify	**Notification under the PPIP Act** • The General Manager (or delegate) will notify the Privacy Commissioner **immediately** after determining that a Data Breach is an Eligible Data Breach or possible Eligible Data Breach. • Notification to the Privacy Commissioner will be made using the approved form, by the Privacy Commissioner as published on the IPC's website and as updated from time to time. • The General Manager (or delegate) and DBRT (if activated) will notify affected individuals as soon as practicable after identifying an Eligible Data Breach. • The General Manager (or delegate) and DBRT (if activated) will determine how to notify and oversee the notification procedure to affected individuals of the Eligible Data Breach in accordance with this Policy. **Notification under the Privacy Act** • The General Manager (or delegate) and DBRT (if activated) will notify the OAIC and any affected individuals as soon as practicable after identifying a Data Breach that it is required to be reported under the Privacy Act. • The General Manager (or delegate) and DBRT (if activated) will determine how to notify and oversee the notification made to the OAIC and any affected individuals by the Data Breach. **Notification of individuals affected by Data Breaches** • Council will notify affected individuals directly, by telephone, letter, email or in person as considered reasonably practicable by General Manager (or delegate) and DBRT (if activated). • Indirect notification - such as information posted on the Council's website, a public notice in a newspaper, or a media release 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 as to the value of the information contained). • Council will maintain a public notification register in accordance with 59N(2) and s59P of the PPIP Act. Council will also maintain an internal register for Eligible Data Breaches. **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, Department of Customer Service, Cyber Security NSW, the Australian Tax Offices etc).

		• The Manager Digital and Customer Information will update Councils internal Data Breach register and external public notification Data Breach register on Council's website are updated after the reporting of all Data Breaches, as it is relevantly required.
5.	**Review**	**Post Incident Review** • The General Manager (or delegate) and DBRT (if activated) will conduct a post incident review to identify any weaknesses in security protocols, policies and procedures. • A post incident review will consider (as relevantly required): o a root cause analysis of the Data Breach o security audit of both physical, technical and cyber security controls o review of Council's risk management policies and procedures o review of training and awareness practices o review of contractual obligations with contracted service providers o consider any other review considerations, recommendations or guidelines published by the IPC or Privacy Commissioner o conduct a Data Breach response assessment to assess Council's response to the Data Breach and identify areas for improvement o determine any final stakeholder communication requirements. • Once the post incident review has been concluded, the General Manager (or delegate) will stand down the DBRT (if activated). **Record Keeping** • The Manager Digital and Customer Information will: o ensure that all evidence and related records for all Data Breaches are stored in Council's internal register o ensure that Council's Public Notification Register is up to date, and complies with the requirements under s59P of the PPIP Act o update appropriate policies and procedures to include key learnings or identified weakness o implement addition security controls if applicable o apply and implement any further training and awareness practices developed from the post incident review

8. ROLES AND RESPONSIBILITIES

8.1 All Council Representatives

All Council Representatives are required to familiarise themselves and comply with this Policy. A breach of the procedures constitutes a breach of the Council's Code of Conduct and may lead to disciplinary action.

8.2 Contract Managers

If a Data Breach is reported to Council by a contractor, this Policy applies to the Data Breach, subject to the terms of any contract, and applicable legislation.

Council's contract managers who manage third party contracts are responsible for ensuring that relevant service providers and agencies understand and comply with this Policy.

Where third party contractors report a Data Breach to Council, the relevant contract may be referred by the Manager Digital and Customer Information to external lawyers to review and determine what action is to be taken. However, this step should not delay Council dealing with the Data Breach in accordance with the steps outlined in this Policy.

8.3 The General Manager or their delegate

In accordance with Section 59G of the PPIP Act, the General Manager (as the head of the agency) is ultimately responsible for the assessment of Data Breaches and mitigation of harm. The General Manager has delegated responsibility of the assessor to Manager Digital and Customer Information.

The Manager Digital and Customer Information is responsible for immediately making all reasonable efforts to contain the Data Breach and must take all reasonable steps to ensure that assessment of the Data Breach is completed with 30 days (unless an extension is granted in accordance section 59K of the PPIP Act).

8.4 Information Technology (IT) Governance Committee / Data Breach response team (DBRT)

The IT Governance Committee was established in 2023 to support Council's Cyber Security Framework, and is Council's designated Data Breach response team (DBRT) as outlined below:

Position	DBRT Role	Responsibilities
General Manager (medium - high risk only)	Agency head	• General advice and oversight • Delegates responsibilities to the Manager Digital and Customer Information (as required).
Manager Digital and Customer Information	Incident Response Leader/Coordinator Data Privacy Officer	• Coordinate the Data Breach response process • Communicate with the General Manager and third parties • Records management • Reporting the Data Breach to regulator such as the Privacy Commissioner
IT Business Partner	IT/Security Specialist	• Identifying the cause of the Data Breach • Containing the Data Breach • Implementing technical controls
Director Community & Customer Service	Operational Management	• Community and customer service liaison • Operational functions of the business • Oversight and advice
Manager Communications and Events	Communication and media liaison	• Media liaison • Managing social media
Director People and Culture	HR and Communication liaison for Council Representatives	• Council Representative impact assessment • Council Representative impact welfare management • Internal communications • Potential Code of Conduct or HR related issues arising from the Data Breach • Internal communications plan
Manager Risk and Compliance	Business continuity advisor Cyber security Insurance Liaison	• Risk analysis and management • Cyber insurance
Independent Advisor (medium - high risk only)	As required based on severity	• Providing appropriate advice and assistance if required.

8.5 Additional expertise

Depending on the severity and nature of the incident, Council, as approved by the General Manager (or delegate) and DBRT (if activated), may engage third parties for additional support or expertise such as legal advice, technical or cyber security service providers.

Other Council Representatives may also be asked to join the DBRT depending of the nature of the Data Breach, at the absolute discretion of the General Manager (or delegate).

9. RELATED POLICIES/PROCEDURES

- Privacy Management Plan
- Cyber Security Policy
- IT Usage and Surveillance Policy
- Cyber Security Incident Response Plan
- Business Continuity Plan.
- IT Disaster Recovery Plan

10. POLICY AUTHORITY

Council.

11. GETTING HELP

For further information regarding this Policy please contact Manager Digital and Customer Information.

12. REVIEW

This Policy to be reviewed annually.

13.ADOPTED BY COUNCIL/EXECUTIVE:

DATE: 23 October 2023
RESOLUTION NO: 222/23

14.VERSION CONTROL TABLE

DATE	VERSION	RES. NO.	KEY CHANGES	AUTHOR
23 October 2023	1.0	222/23	New Policy	Jade Reed, Manager Digital and Customer Information