POLICY TITLE:	**DATA BREACH NOTIFICATION POLICY**
FOLDER NUMBER:	F2007/00307
POLICY OWNER / DIVISION:	Corporate Support Division
POLICY OWNER / BRANCH:	Governance and Customer Service
FUNCTION:	Governance
RELEVANT LEGISLATION:	*Part 6A of the* Privacy and Personal Information Protection Act 1998 *(NSW) (**PPIP Act**)*
POLICY ADOPTION/AMENDMENT DATE:	9 April 2025 **REPORT NUMBER**: CS3/25
REVIEW YEAR:	2027
AMENDMENT HISTORY:	
RELATED POLICIES:	Statutory- Privacy Management Plan

POLICY PURPOSE / OBJECTIVES:

POLICY STATEMENT:

The PPIP Act sets out that public sector agencies including Councils, notify the NSW Information and Privacy Commission (IPC) and individuals affected by data breaches involving personal or health information likely to result in serious harm to an individual to whom the information relates.

Not all data breaches require notification to take place. After assessment arranged by the Privacy Officer, a breach will be reported to the IPC if it is deemed notifiable.

This process must take place as soon as the breach has been brought to the attention of the Privacy Officer and assessed. This must be completed within 30 days. The assessment must identify the necessary steps to be taken, they must be documented and actioned.

Hornsby Shire Council Data Breach Notification Policy

1. Purpose

This policy outlines the procedures for managing and responding to data breaches involving personal information held by Hornsby Shire Council. The aim is to ensure that data breaches are identified, contained, investigated, and reported promptly to mitigate potential harm to individuals and comply with legal obligations

under the NSW Information and Privacy Commission (IPC) Office of the Australian Information Commissioner (OAIC) using the Mandatory Notification of Data Breaches (MNDB) Scheme.

2. Scope

This policy applies to all employees, contractors, and third-party service providers of Hornsby Shire Council who handle personal information.

3. Definition of a Data Breach

A data breach occurs when personal information held by the Council is lost or subjected to unauthorized access, modification, disclosure, or other misuse. Examples include:

- Loss or theft of physical devices containing personal information.
- Hacking or other forms of unauthorized access to Council systems.
- Accidental disclosure of personal information to unauthorized individuals.

4. Responsibilities

- **Employees and Contractors**: Must report any suspected or actual data breaches to their supervisor or the designated Privacy Officer (PO) Data Protection Officer (DPO) immediately.
- **Council's Privacy Officer (PO)**: Responsible for managing the response to data breaches, including arranging assessment, containment, investigation, and notification.

5. Data Breach Response Plan

5.1 Identification and Reporting

All suspected or actual data breaches must be reported immediately to the PO and include the following:

- A description of the type(s) of personal information involved
- How many separate individuals/ parties/ agencies were involved in the breach
- How many of the individuals/ parties/ agencies have been notified of the breach
- Was it a cyber incident?
- Provide an estimate of the financial implications of the breach to Council
- The PO will log the incident and arrange a preliminary assessment to determine the severity and impact of the breach in accordance with the MNDB Scheme

5.2 Containment and Assessment

- The PO will take immediate steps to contain the breach and prevent further unauthorized access or disclosure.
- An assessment will be conducted to determine the nature and extent of the breach, including the type of personal information involved, the cause of the breach, and the potential impact on affected individuals.

5.3 Detailed Breach Assessment

- **Nature of the Breach:** Identify how the breach occurred, including whether it was accidental or malicious, and the specific vulnerabilities that were exploited.
- **Type of Personal Information Involved:** Determine the categories of personal information affected, such as names, addresses, financial information, health records, etc.
- **Scope of the Breach:** Assess the number of individuals affected and the extent of the data exposure.
- **Potential Harm:** Evaluate the potential harm to individuals, including risks of identity theft, financial loss, reputational damage, and emotional distress.
- **Mitigation Measures:** Identify immediate steps taken to mitigate the impact of the breach, such as disabling compromised accounts, recovering lost data, and enhancing security measures.

5.4 Notification

- If the breach is likely to result in serious harm to individuals, the PO will notify the affected individuals as soon as practicable.
- The notification will include:
    - A description of the breach.
    - The type of personal information involved.
    - Steps taken to contain and mitigate the breach.
    - Recommendations for individuals to protect themselves.
    - Contact details for further information and assistance.
- The PO will also notify the NSW Information and Privacy Commission (IPC) and Office of the Australian Information Commissioner (OAIC) if the breach meets the criteria for mandatory reporting under the Privacy Act 1988.

5.5 Review and Prevention

- Following the resolution of the breach, the PO will arrange an investigation to address issues that led to the breach
- Review and update relevant policies and procedures if necessary to help prevent future breaches.
- Carry out a security audit of processes and controls involved to ensure all employees and contractors (if applicable) understand their responsibilities regarding data protection.
- Update the IPC if any further new information about the breach becomes available.

6. Policy Review

This policy will be reviewed every two years or following a significant data breach to ensure its effectiveness and compliance with legal requirements.

7. Contact Information

For any questions or concerns regarding this policy, please contact the Privacy Officer/ Manager, Governance and Customer Service at 9847 6761.