Attachment 1 to Item 10.4.3.

Draft Data Breach Policy

Date of meeting: 26 November 2024
Location: Council Chambers
Time: 6:30pm

Data Breach

DRAFT COUNCIL POLICY

Division:	Corporate Services	**Policy Number:**	
Branch:	Governance and Risk	**Adopted Date:**	
Responsible Officer:	Manager Governance and Risk	**Next Review Date:**	
Director:	Director Corporate Services	**Version:**	1

Table of Contents

1. TITLE

Data Breach Policy.

2. PURPOSE

The purpose of this Policy is to document Council's plan when responding to data breaches of personal or health information under Commonwealth and State legislation.

3. SCOPE

This Policy applies to all data held by Council in any Council record, in physical or electronic format.

This Policy applies to all Council officials, including Councillors, Councils staff members, administrators, Council Committee members, delegates of Council, contractors, and volunteers.

This Policy includes data breaches as identified under the Commonwealth Notifiable Data Breaches (NDB) Scheme, data breaches under the Mandatory Notification of Data Breach (MNDB) Scheme, and any other data breach of personal or health information as described under the Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act).

Council staff should read the Data Breach Response Plan in conjunction with this Policy.

4. BACKGROUND

The NDB Scheme was introduced as an amendment to the Australian Privacy Act 1998, and it requires subject entities to undertake actions to prevent, investigate and report incidents where personal information is accessed without authorisation in a way that is likely to cause harm.

Council was identified as an organisation that is a tax file number recipient and was required to create a Data Breach Response Plan that identifies actions to be taken only when there are data breach incidents involving tax file numbers under the NDB Scheme. It was received by the Audit Committee at its meeting on 20 June 2018.

Amendments were made to the Privacy and Personal Information Protection Act 1998 (PPIP Act) that are effective from 28 November 2023. They require agencies to provide notifications to affected individuals in the event of an eligible data breach of their personal or health information by a NSW public sector agency.

An amendment to the PPIP Act includes the creation of the MNDB Scheme which involves the requirement of agencies to have a publicly accessible data breach policy.

5. POLICY DETAILS

Preparing for a Data Breach

Cyber Response

5.1 Council's cyber response includes:

- Administering regular audits of Council's data and information storage systems
- Regularly testing the security of the systems
- Proactive incident planning and staff training.

Incident Management

5.2 A data breach incident will be managed by Council's Manager Governance and Risk (as Council's Privacy Contact Officer) or another and the Data Breach Response Team (see Appendix 1). They will be responsible for carrying out and following the actions outlined in this Policy and the Data Breach Response Plan.

Communication Strategy

5.3 The communication strategy involves three stages: notifying the breach to the relevant regulatory agency, notifying affected individuals/organisations, reporting to other relevant external agencies. The assessor will be responsible for implementing the three stages.

5.4 If a data breach incident occurs, the assessor will be responsible for any mandatory reporting to organisations, such as the Information Privacy Commission (IPC), and any external consultation that is required in line with this Policy.

5.5 Depending on the type and severity of the data breach incident, the assessor can escalate Council's response to the data breach to the Data Breach Response Team. Council's Corporate Communications and Customer Experience Branches may then develop a strategy for notifying affected people and organisations following protocols outlined in the Data Breach Response Plan.

5.6 Depending on the types of information involved in the breach, the severity of the breach, and the number of individuals or organisations impacted by the breach, the communication channels that could be used include: email notification, direct mail, phone call, website announcement, social media or press release.

5.7 The key contact in Council regarding a data breach is:

Title: Manager Governance and Risk
Email: council@hawkesbury.nsw.gov.au
Phone: (02) 4560 4444.

Risk Management

5.8 During the post data breach review period, any risks identified during the data breach incident will be added to Council's Enterprise Risk Register and a mitigation strategy will be implemented. Council's risks are regularly reviewed and have oversight by the Audit, Risk and Improvement Committee.

Key Controls

5.9 Council has key controls to help prevent and mitigate data breach incidents. These include, but are not limited to:

- Access controls to limit access to sensitive or confidential information
- Firewalls to prevent unauthorised access
- Security awareness training for all staff
- Data backup and recovery processes so that information can be restored if lost
- Compliance with data security and protection regulations and standards.

Training and Awareness

5.10 Council endeavours to manage a well-trained and aware workplace by implementing privacy training and awareness strategies, including:

- Regular security training with routine simulation tests, and re-testing when required
- Providing access to this Policy and other relevant policies, such as the Privacy Management Plan
- Participating in Privacy Awareness Week and providing internal communications to staff
- Including privacy and data breach information during the induction process
- Running tests to ensure that Council's security measures can identify data breaches and that the Data Breach Response Plan sufficiently captures the processes for responding to a data breach.

5.11 Using resources provided by organisations such as the IPC and Cyber Security NSW, the staff responsible for managing data breaches will keep abreast of current practices and methodologies to assess breaches as efficiently and effectively as possible. Where there are gaps in knowledge, external advice will be sought from relevant agencies and organisations.

Data Breaches

What is a data breach?

5.12 The unauthorised access or disclosure of personal information, or loss of personal information.

5.13 A data breach may be deliberate or accidental, and may occur by a range of different means, including, but not limited to:

- Human error
  - When a letter or email is sent to the wrong recipient
  - When system access is incorrectly granted to someone without appropriate authorisation
  - When a physical asset such as a paper record, laptop, USB stick or mobile device containing personal information is lost or misplaced
  - When staff fail to implement appropriate password security, such as not securing passwords or password sharing
- System failure
  - Where a coding error allows access to a system without authentication, or results in automatically generated notices that include the wrong information or are sent to the incorrect recipients
  - Where systems are not maintained through the application of known and supported patches
- Malicious or criminal attack
  - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information
  - Social engineering or impersonation leading to inappropriate disclosure of personal information
  - Insider threats from Council employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions
  - Theft of a physical asset such as a paper record, laptop, USB stick or mobile device containing personal information.

What is an eligible data breach under the NDB Scheme?

5.14 The unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates.

What is an eligible data breach under the MNDB Scheme?

5.15 When there is unauthorised access to, or unauthorised disclosure of, personal information held by Council and that access or disclosure would likely result in serious harm to the individual to whom the information relates.

5.16 When personal information held by Council is lost in circumstances where:

- Unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and
- If the unauthorised access, or unauthorised disclosure of, the information was to occur, the access or disclosure would likely result in serious harm to the individual to whom the information relates.

5.17 An eligible data breach may include the following:

- A data breach that occurs within Council
- A data breach that occurs between Council and another public sector agency
- A data breach that occurs by an external person or entity accessing data held by Council without authorisation.

Identifying and Reporting Data Breaches

5.18 Council has various processes in place to identify or preventing a data breach, including:

- Physical data breaches:
  - Security cameras
  - Reviewing key access
  - Physical file tracking
- Electronic data breaches:
  - Detection systems
  - System monitoring
- External or internal audits or reviews
- Staff training and awareness.

5.19 If you are a Councillor, Council worker or contractor, and suspect or are aware of a data breach, you can notify the General Manager (or delegate), or your supervisor or direct contact within Council who will then be responsible for notifying the General Manager (or delegate).

5.20 If you are external to Council and suspect a data breach has occurred, you can report the data breach to the General Manager. The General Manager can be contacted at:

Email: council@hawkesbury.nsw.gov.au
Phone: (02) 4560 4444.

5.21 When reporting, you should include as much information as possible, including:

- The time and date that the suspected breach was discovered
- The type of information involved
- The suspected cause and extent of the breach
- Any other background about the compromised information which may affect the consequences of the breach.

Managing Data Breaches

Assessment of Breach Reports

5.22 Upon receipt of a report of a data breach, the General Manager (or delegate) must direct an assessor (generally the Manager Governance and Risk or external assessor engaged by Council) to carry out an assessment of the suspected data breach in accordance with Council's Data Breach Response Plan and take any immediate action to mitigate known risks. The assessment must be completed within 30 calendar days of the person becoming aware of the breach. See Appendix 2 for a summary view of Council's assessment process.

5.23 Each report of a data breach will be assessed on a case-by-case basis and will look at the following factors:

- The types of information involved in the breach
- The sensitivity of the information involved in the breach
- Whether the information is or was protected by security measures
- The persons to whom the unauthorised access to, or unauthorised disclosure of, the information involved in the breach was, or could be, made or given
- The likelihood that this person has or had the intention of causing harm or if they did or could circumvent security measures protecting the information
- The nature of the harm that has occurred or may occur.

5.24 The purpose of assessing a report of a suspected data breach is to:

- Confirm if a data breach has occurred
- Perform an analysis of all information gathered about the breach to evaluate the scale, scope, content and potential impact on affected individuals
- Determine if the data breach falls under the scope of an eligible data breach under the NDB or MNDB Schemes and report the incident to the IPC or Office of the Australian Information Commissioner (OAIC) if it is.

Containment of Breach

5.25 Once a data breach has been reported and during the assessment of the breach, Council will take all necessary steps to contain the breach and mitigate the harm caused by it. Steps will be taken to prevent the affected information from being accessed further, and to prevent any other information from being breached. This could involve:

- Recovering the lost or stolen information
- Isolating and/or shutting down the systems that were breached
- Revoking access to systems
- Patching identified system vulnerabilities
- Preserving evidence of the breach.

Risk Evaluation of Breach

5.26 A risk assessment of the data breach will be conducted to evaluate the information involved and determine the harm caused by the breach. The risk assessment will include consideration of:

- Who is affected by the data breach and if their circumstances put them at particular risk of harm
- The cause of the data breach to determine if it was a targeted attack or the result of a system flaw
- The foreseeable harm to the affected parties and if it constitutes a case of 'serious harm' under this Policy
- If there is cause to escalate the data breach to the Data Breach Response Team e.g., if the information was particularly sensitive, who the information was exposed to, the risk of harm, the number of individuals affected.

Notification and Reporting of Breach

5.27 If a data breach occurs, Council will take all necessary steps to mitigate any harm caused by the breach. This will include notifying affected individuals and organisations as soon as practicable, with limited exceptions.

5.28 The decision to notify will be made by the General Manager (or delegate) based on advice from the assessor and in consultation with the Data Breach Response Team as necessary.

5.29 The notification options include:

- Notifying all individuals and organisations affected by the data breach, unless there is an exemption
- In cases where the data breach is an eligible data breach under the NDB Scheme or MNDB Scheme, Council will:
  - Notify the OAIC for breaches under the NDB Scheme
  - Notify the Privacy Commissioner for breaches under the MNDB Scheme
- In cases where Council is unable to, or if it is not reasonably practicable to notify any or all individuals and organisations affected by a data breach, Council will publish a notification in the public notification register.

5.30 After assessing the breach Council can decide not to notify affected parties if:

- The breach involves more than one public sector agency and another agency involved in the same breach notifies the affected parties
- The notification would likely prejudice any investigation or legal proceedings
- Council successfully contains the breach and limits the likelihood that you will experience serious harm
- There are overriding secrecy provisions in other laws that prohibit or regulate the use or disclosure of the relevant information
- Notification would create a serious risk of harm to an individual's health or safety
- Notification would worsen Council's cybersecurity or lead to further data breaches.

5.31 Depending on the circumstances of the data breach and the categories of data involved, the General Manager (or delegate) in consultation with the assessor and Data Breach Response Team will determine if Council needs to notify or engage with other agencies. For a list of organisations, see Appendix 3.

Post-Breach Review and Evaluation

5.32 After a data breach has been managed, a review of the incident will be conducted by the assessor and the Data Breach Response Team, if required, and reported to the General Manager to:

- Evaluate Council's management of the incident and find improvements to the process and this Policy and the Data Breach Response Plan
- Determine what preventative measures can be taken to ensure a similar breach does not occur again, e.g., audits of Council's security controls, reviewing Council's practices and processes
- Control any other risks that were identified during the incident that need to be mitigated by Council.

5.33 The post-breach review will cover:

- The effectiveness of this Policy and the Data Breach Response Plan
- A root cause analysis of the data breach
- If required, more focused reviews of particular systems, policies and procedures involved in the breach, for example:
  - Council's data retention and disposal processes
  - Making a manual process more safe
  - A security review
  - Reviewing contractual arrangements
- An assessment of how the breach has impacted other Council policies and procedures and potential amendments to be made.

Recordkeeping Responsibilities

5.34 All records created that relate to the data breach must be registered in Council's records management system in accordance with Council's Records Management policy, including:

- The report of the breach
- The assessment of the breach
- The containment of the breach
- The risk evaluation of the breach
- The notifications of the breach
- The post-incident review of the breach
- Any reports Council has made of the breach to other agencies.

5.35 Under the PPIP Act, Council has to maintain two data breach registers:

- A public notification register to be published on Council's website that includes information such as the date of the breach, a description of the breach, the personal information that was subject of the breach, actions taken to mitigate the harm done by the breach etc.
- An internal data breach incident register that includes information such as the type of data breach, who was notified of the breach, when the breach was notified, actions taken to mitigate harm done by the breach, the estimated cost of the breach etc.

Policy Review and Testing

5.36 To ensure this Policy remains effective and current, it will be reviewed annually. The review will consider:

- Any suggested improvements that come out of a post-breach review
- Any changes that have occurred in Council's internal or external environment
- The results of annual internal testing of this Policy and the Data Breach Response Plan
- Amendments to legislation and updates to advice from regulatory bodies, e.g., the Information Privacy Commission.

5.37 The review of this Policy will include a review of related policies and procedures to ensure that they are aligned with each other, for example, the Privacy Management Plan, Data Breach Response Plan and cyber security policies and procedures.

Third Parties

5.38 Council conducts business with various other organisations, contractors and third parties, and a breach of Council's data could occur through these channels. Council's contracts and agreements with third parties will include provisions about complying with privacy legislation, including the management, notification, and remediation of data breaches.

5.39 If a data breach occurs, Council will:

- Set up a communication channel with the affected party
- Assess the incident to determine if any critical Council information was involved and which Council systems are at risk
- In collaboration with the affected party, determine who will be responsible for the overall management of the data breach and notification processes (if required).

5.40 In the event that a suspected or actual data breach occurs, the third party can notify their main point of contact within Council who will be responsible for notifying the General Manager (or their delegate), or they can notify the General Manager directly.

5.41 If a Council email address is detected in a third-party breach, affected staff members will be notified and provided with mitigation strategies e.g., changing their password.

6. ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Council Officials	• Protect personal information against loss or unauthorised access or disclosure. • Report suspected data breaches to the General Manager or their supervisor following guidance in this Policy and Data Breach Response Plan. • Recordkeeping responsibilities.
General Manager (or their delegate)	• Receive reports of suspected data breaches. • Select an assessor (generally the Manager Governance and Risk) to assess reports of suspected data breaches.
Data Breach Assessor	• Assess reports of suspected data breaches. • Notify the Information Privacy Commission and OAIC when an eligible data breach has occurred. • Determine if a data breach requires escalation to the Data Breach Response Team and convene the Data Breach Response Team. • Conduct post-breach reviews and evaluations. • Provide advice and report back to the General Manager and Executive Team regarding the data breach. • Manage communications regarding third party breaches.
Manager Governance and Risk (Privacy Contact Officer)	• Maintain the public notification register and internal data breach incident register. • Review, manage and test this Policy. • Add any identified risks from a data breach incident to Council's Enterprise Risk Register and implement mitigation strategies.
Manager Corporate Communications and Events	• Carry out and review the communication strategy in relation to public notification processes accordance with this Policy and the Data Breach Response Plan.
Data Breach Response Team	• Provide advice to the assessor. • Manage and respond to a data breach in accordance with the Data Breach Response Plan.

7. DEFINITIONS

Assessor	An employee of Council or an employee from another government agency or third party acting on behalf of Council who is responsible for carrying out an assessment of a suspected data breach
Council Official	Councillors, members of the staff of Council, Committee members, contractors, consultants and volunteers representing Council in an official capacity
Loss (of personal information)	When personal information is removed from the possession or control of Council. Loss may occur because of a deliberate or accidental act or omission of Council, or due to the deliberate action of a third party.
MNDB Scheme	The NSW Mandatory Notification of Data Breach Scheme
NDB Scheme	The Commonwealth Notifiable Data Breaches Scheme
Personal Information	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 whose identity is apparent or can reasonably be ascertained from the information or opinion
Serious Harm	Harm that may entail physical, psychological, emotional, financial, or reputational damage. For harm to be likely to occur, the risk of harm must be more probable than not, rather than just being possible. It has to be harm that is weighty or grave, and not trifling or transient.
Unauthorised Access	When personal information held by Council is accessed by an individual who does not have the necessary permissions or authority, including internal access by a Council official, or external access by a third party
Unauthorised Disclosure	When personal information is made accessible or visible to individuals outside of Council, intentionally or unintentionally, in a manner that is not permitted under the Privacy and Personal Information Protection Act 1998 or the Health Records and Information Privacy Act 2002

8. RELATED DOCUMENTS

Legislation

- Privacy and Personal Information Protection Act 1998
- Health Records Information Privacy Act 2002
- Australian Privacy Act 1998
- Privacy Code of Practice for Local Government

Related policies

- Council's Code of Conduct
- Privacy Management Plan
- Cyber Security Corporate Policy

Procedures

- Data Breach Response Plan
- Records Management OMS

Guidelines

- IPC's Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy, May 2023

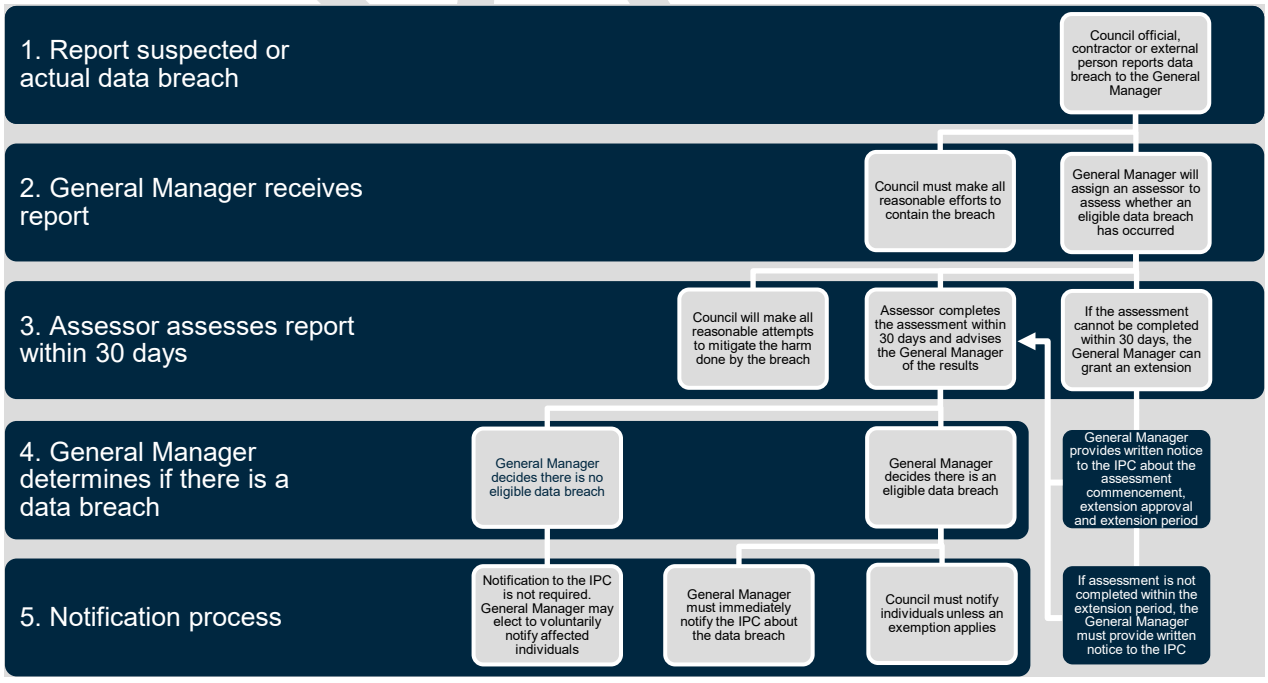
9. APPENDICES

Appendix 1 – Data Breach Response Team

The Data Breach Response Team are responsible for responding to a data breach under this Policy and for following the Data Breach Response Plan. Some or all of the staff members listed below may be required to respond to a data breach. The assessor will be responsible for determining who is required.

Officer	Responsibility
Manager Governance and Risk	Overall management of the data breach and providing privacy expertise; risk management
Manager Corporate Communications and Events (or delegate)	Media and communications
Legal Counsel	Legal support
Manager Information Services (or delegate)	Required if the breach is related to IT and provision of IT support
Manager People and Development (or delegate)	Required if the breach involves a member of staff
Coordinator Facilities Operations (or delegate)	Required if the breach involves the physical security of Council
Manager Business Transformation and Customer Experience (or delegate)	Required if the breach could involve a large community response and customer experience support

Appendix 2 – Summary of data breach assessment process



Appendix 3 – List of agencies to report data breach incidents to

Agency	Reason for Notification	Reporting
Privacy Commissioner	If a data breach is an eligible data breach under the MNDB Scheme, then it must be reported to the Privacy Commissioner in accordance with the Data Breach Response Plan.	Mandatory
Office of the Australian Information Commissioner	If a data breach is an eligible breach under the NDB Scheme, then it must be reported to the OAIC in accordance with the Data Breach Response Plan.	Mandatory
NSW Police Force	If assessment of a data breach identifies that the cause of the data breach is cybercrime or other theft, the NSW Police need to be notified in order to investigate the crime.	Mandatory
Cyber Security NSW	Involving Cyber Security NSW can have the following benefits: • Providing guidance on mitigation measures and methods to enhance Council's data security • Assessing risks to understand how the public can be protected • Using the information about the breach to analyse trends and patterns.	Discretionary
Australian Taxation Office	If a data breach included personal information that has compromised someone's tax identity, it should be reported to the Australian Taxation Office so that they can place protective measures on client accounts.	Mandatory
Australian Federal Police	If assessment of the data breach identifies that the cause of the data breach is cybercrime or other theft, the Australia Federal Police may need to be notified in order to investigate the crime (could be an escalation from the NSW Police).	Discretionary
Office of the Government Chief Information Security Officer	If a data breach is a result of a cyber security incident, it can be reported to the Chief Information Security Officer. They can assess the impact to Council and oversee any incident response activities.	Discretionary
Australian Cyber Security Centre	If a data breach is a result of a cyber security incident, it can be reported to the Australian Cyber Security Centre / Australian Signals Directorate.	Discretionary
Affected third party organisations / agencies	If a data breach affects a third party organisation or agency, they should be notified so they can conduct their own assessment to determine if they have also experienced a data breach and to help manage the breach from their end.	Mandatory
Financial services providers	If a data breach affects Council's financial service providers, or could have an impact on Council's finances, then they should be notified.	Mandatory

Professional associations or regulatory bodies	If a data breach could have implications for other councils, it could be beneficial to notify a relevant professional association or regulatory body.	Discretionary
Insurer	Data breach incidents should be reported to Council's insurer so they are aware of the potential risks to Council.	Mandatory