Inc.1874

Burwood

Burwood . Burwood Heights . Croydon . Croydon Park . Enfield . Strathfield

DATA BREACH POLICY

PO Box 240, BURWOOD NSW 1805
2 Conder Street, BURWOOD NSW 2134
Phone: 9911-9911 Fax: 9911-9900
Email: council@burwood.nsw.gov.au
Website: www.burwood.nsw.gov.au

Public Document
Adopted by Council: 13 February 2024 (Min. No. 8/24)
Ref. No.: 23/47675
Version No.: 1
Joint Ownership: Governance & Risk and Information Technology

1. Purpose

This policy has been adopted to inform the public of Council's approach to identifying, responding to and reporting data breaches of Council held information.

The objective of this Policy is to set out Council's approach to identifying and managing a data breach, including:

- providing examples of situations considered to constitute a data breach
- outlining the key steps involved in responding to a data breach
- outlining 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,
- assisting Council in avoiding or reducing possible harm to both the affected individuals and the Council.

This Policy will assist the Council to meet its legal obligations in respect of Mandatory Reporting Data Breaches under the NSW *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the Commonwealth *Privacy Act 1988* and complies with best practice guidelines.

2. Scope

This policy is applicable to all council officials. A breach of this policy constitutes a breach of the Council's *Codes of Conduct* and may lead to disciplinary action.

This policy applies to all data breaches of information held by Burwood Council in either a paper based or electronic format. Council holds personal information such as ratepayer, resident and customer data and personal or commercial information from parties who interact with Council. Council also maintains personnel and workforce information. This data is collected by Council and is used to plan, monitor and manage the workforce, services and properties across the Local Government Area.

This policy supplements Council's *Privacy Management Plan*, which provides more information on how Council may collect, use and disclose personal information.

3. Background

The Notifiable Data Breaches (NDB) scheme came into effect under the *Privacy Act 1988* of the Commonwealth (Privacy Act) in February 2018. Under the NDB, scheme organisations must notify affected individuals and the Office of the Australia Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information has been compromised.

In addition to the NDB scheme, amendments to the *Privacy and Personal Information Protection Act 1998* of NSW (PPIP Act) taking effect on 28 November 2023 create a Mandatory Notification of Data Breach (MNDB) Scheme that requires public sector agencies bound by the PPIP Act to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Council must comply with the notification requirements of the scheme in the event of any data breach occurring, as failure to do so may render Council liable for significant penalties under Australian law.

4. Definitions

Commercial information	Any commercial information, whether it be that of Council, external stakeholders' or provided by a service provider in confidence. Note that commercial information does not fall within the MNDB scheme unless it contains Personal Information or Health Information, but it is information that Council also strives to protect.

Council official	Councillors, employees and delegates (including volunteers, consultants, contractors or any other service provider involved in exercising a Council function).
CSIRT	Means the Cyber Security Incident Response Team established under Council's Cybersecurity Incident Response Plan.
Data breach	See section 5 of this policy.
Eligible data breach	See section 6 of this policy.
General Manager	A reference in this policy to the "General Manager" includes a reference to a delegate of the General Manager under this policy.
Harm	See section 6 of this policy.
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.
IPC	Means the NSW Information and Privacy Commission.
MNDB	Means the Mandatory Notification of Data Breaches Scheme established under Part 6A of the *Privacy and Personal Information Protection Act 1998* of NSW.
NDB	Means the Notifiable Data Breach scheme established under the *Privacy Act 1988* of the Commonwealth.
Officer	For the purposes of this policy, any reference to the term "officer" is taken to mean all Council officials other than councillors or administrators who are involved in exercising a council function.
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 Act	Means the *Privacy Act 1988* of the Commonwealth.
PPIP Act	Means the *Privacy and Personal Information Protection Act 1998* of NSW.
Unauthorised access	See section 5 of this policy.

5. What is a data breach?

A ***data breach*** is an incident where unauthorised access to, or unauthorised disclosure or loss of, personal information or health information has occurred. The information may have been compromised, disclosed, copied, transmitted, accessed, removed, or destroyed.

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 cyberattack has occurred, which has resulted in personal information being stolen.

Unauthorised access to personal information occurs when personal information held by an agency is accessed by someone who is not permitted to do so. Unauthorised access can occur:

- **Internally within an agency** – for example, an employee browses agency records relating to another employee or a family member without a legitimate purpose.
- **Between agencies** – for example, a team at one agency may be provided with access to systems and data at a second agency as part of a joint project. Unauthorised access may occur if a member of that team were to use that access beyond what is required for their role as part of that project.
- **Externally outside an agency** – for example, personal information is compromised during a cyberattack and accessed by a person external to the agency.

6. Responsibilities

The ***Manager Governance & Risk*** and the ***Manger Information Technology*** are jointly responsible for implementation of this policy.

All council officials, service providers and members of the public are responsible for immediately reporting any actual or suspected data breaches to the Manager Information Technology, Manager Governance & Risk or Director Corporate Services.

The ***Cyber Security Incident Response Team***, in addition to its responsibilities under Council's *Cybersecurity Incident Response Plan*, is also responsible for the following in relation to eligible data breaches under this policy:

- Immediately meeting to review and respond to the reported data breach, with delineation of responsibilities undertaken depending on the nature of the data breach.
- Following the response requirements as set out in this Data Breach Policy.
- Consulting with relevant internal and external stakeholders as required.
- Assisting the General Manager with notification requirements.

The ***General Manager*** or their delegate is responsible for reporting eligible data breaches to the appropriate bodies in accordance with section 10 of this policy.

7. Identifying and reporting breaches

Council may be made aware of a data breach through a report from an officer, a contractor, an affected third party, a member of the public, or through a report from another government agency.

Data breaches may also be identified as a result of investigations into Council's IT infrastructure or cybersecurity incidents such as malware, hacking, ransomware, phishing or a combination of these. Council has in place a number of internal policies and procedures to manage cybersecurity risks including the *Cyber Crime and Security Incident Corporate Practice* and *Cybersecurity Incident Response Plan*, which requires certain incidents to be reported immediately to the Manager Information Technology.

Council has in place a Cyber Security Incident Response Team (CSIRT) that investigates data breaches that arise from cyber incidents. The Manager Governance & Risk is a member of the CSIRT and, as the officer responsible for Council's *Privacy Management Plan*, brings that expertise and responsibility to the CSIRT's assessment of data breaches that may also be eligible data breaches under this policy.

In the event of a known or suspected data breach relating to personal information or health information that arises from a non-cyber incident, this should be reported either verbally or in writing to Council's Manager Governance & Risk or Director Corporate Services, as soon as

practicable, for assessment in accordance with this policy and Council's *Privacy Management Plan*.

8. When does a breach become 'eligible' for notification?

Under the Mandatory Notifiable Data Breach (MNDB) scheme Council must notify affected individuals and the NSW Privacy Commissioner about an eligible data breach.

An ***eligible data breach*** occurs where:

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.

Harm caused by a breach can be assessed in number of ways and may be determined based on the following factors:

- Physical safety of the person or organisation
- Financial loss
- Emotional wellbeing or loss
- Reputational damage
- Legal liability
- Breach of secrecy provisions.

In relation to the NDB under the Privacy Act, Council must notify the Australian Information Commissioner of instances where a data breach affects the tax file number of individuals.

9. Data Breach Preparation and Prevention Measures

Council maintains a risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation in accordance with AS ISO 31000:2018.

Council also has a range of supporting policies to control and mitigate exposures to breaches of data. This includes a Business Continuity Plan, Fraud and Corruption Control Policy, Privacy Management Plan and Codes of Conduct.

In addition to the policy controls, Council has a comprehensive set of information technology and cyber security controls. This includes robust access controls, data encryption, network and endpoint security measures, data loss prevention systems, and incident response plans. An up-to-date inventory of assets is maintained, along with strong patch and vulnerability management measures, to ensure all IT assets are properly secured and monitored. Regular penetration tests are performed by a third party to identify and remediate any weaknesses in the IT infrastructure.

Other measures Council undertakes to minimise the risks of data breaches and ensure appropriate response in the event of a breach are:

- Council officials are provided with an IT induction and receive a copy of the Data Breach Policy when they commence a role at Council and the information is constantly available to employees on Council's intranet and to Councillors on the Councillor Portal.
- Provides training and targeted advice to council officers and business units to help them understand how the Data Breach Policy is implemented.
- Encourages Council officials to seek advice from the relevant officers in Council in relation to any potential data breach issues or concerns.
- Promotes awareness and compliance with Data Breach requirements by participating in promotional activities as part of the annual Privacy Awareness Week and Cybersecurity Awareness Month.

- Ensures that service providers are aware of their obligations under this Policy to report any data breaches to either the Manager Information Technology, Manager Governance & Risk or Director Corporate Services immediately.
- Schedules regular testing to assess the effectiveness of Council's response to data breaches, and to assess whether there are any risks that need to be addressed.

10. Data breach response strategy

Council's data breach response utilises the existing CSIRT structure and processes to investigate, respond and report internally on any suspected eligible data breach. It is noted the CSIRT will have concurrent responsibilities and actions in relation data breaches arising from a cybersecurity incident.

The data breach response involves the following steps, some of which may occur concurrently.

Step 1 — Report and triage

Any Council Officer who becomes aware of a Data Breach will immediately notify the Manager Information Technology, Manager Governance & Risk or Director Corporate Services.

Where either of those Managers believe, or have reasonable grounds to believe, that the data breach is an eligible data breach, that Manager will notify the General Manager (or delegate) immediately.

Step 2 — Contain

Containing the data breach will be prioritised. All Council officers will take all immediate steps to contain any data breach by limiting the extent and duration of the unauthorised access to or disclosure of Council held Information, and preventing the data breach from intensifying. This obligation is ongoing as other steps proceed.

If a third party is in possession of the personal information and declines to return it, it may be necessary to seek legal or other advice on what action can be taken to recover the information. When recovering information, Council will make every attempt to ensure that copies have not been made by a third party or, if they have, that all copies are recovered.

Step 3 — Assess and Evaluate

To determine what other steps are needed, an assessment of the type of information involved in the suspected breach and the risks associated with the breach will be undertaken. The General Manager (or delegate) will appoint a member of the CSIRT to conduct that assessment.

Assessment of the breach should be completed as soon as practicable and at latest within 30 calendar days of the breach being reported.

Factors to consider when conducting the assessment include:

- What is the nature of the information that has been lost or disclosed? Some types of information are more likely to cause harm if compromised.
- 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 may 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.
- Did the data breach involve tax file number 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 or organisations?
- Who is in receipt of the Council held information?
- What is the risk of further access, use or disclosure, including via media or online?
- Are other public agencies involved in the Data Breach?

In conducting the assessment, regard is to be had to any guidelines on the assessment of data breaches published by the IPC.

If the assessment indicates that an eligible data breach has occurred, the General Manager (or delegate) will decide whether an eligible data breach has actually occurred.

The General Manager (or delegate) will also assess and consider whether a data breach is a Commonwealth notifiable data breach.

Step 4 – Notification

If the General Manager (or delegate) decides that an eligible data breach has occurred, the notification process under Division 3 of Part 6A of the PPIP Act is triggered.

The General Manager (or delegate) will take the following actions:

- **Notify the NSW Privacy Commissioner:** immediately notify the NSW Privacy Commissioner about the breach using the approved form published on the IPC website.
- **Determine whether an exemption applies:** If one of the six exemptions set out in Division 4 of Part 6A of the PPIP Act applies in relation to an eligible data breach, Council may not be required to notify affected individuals. This assessment should occur as part of or immediately following the assessment of the data breach.
- **Notify individuals:** Unless an exemption applies, Council will notify affected individuals as soon as reasonably practicable. Notification will be made directly to the individual concerned, their parent or guardian (in the case of children) or an authorised representative. Where Council is unable to notify directly or it is not reasonably practicable to do so, a public notification will be made and advice will be provided to the NSW Privacy Commissioner on how to access that public notification. Where a data breach is not an eligible data breach, Council may still provide voluntary notification to individuals and organisations where appropriate.
- **Provide further information to the NSW Privacy Commissioner (as required):** Agencies may be required to provide additional information to the Privacy Commissioner, if they have been unable to provide complete information in their initial notification, if they have made a public notification, or if they are relying on an exemption.
- **Notifiable data breach under Privacy Act:** Where the data breach is a notifiable data breach under the Privacy Act, the General Manager (or delegate) will notify the Australian Information Commissioner using the approved form published on the website of the Office of the Australian Information Commissioner.
- **Notification to other agencies:** Depending on the circumstances of the data breach and the categories of data involved, Council may need to notify or engage with other agencies. Examples include the NSW Police Force, Cyber Security NSW, Australian Federal Police, Australian Taxation Office and the Department of Health.

Step 5 – Review and monitoring

After the incident has been assessed and notification has taken place, the Manager Information Technology, Manager Governance & Risk and Director Corporate Services 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. This will mitigate future risks and ensure Council's proactive management of data breaches.

The investigation findings and recommendations must be reported to the Executive Team and Council's Audit Risk and Improvement Committee and cover the following:

- Recommended changes to system and physical security.
- Recommend changes to any Council policies or procedures.
- Revision or changes recommended to staff training and education.
- Disciplinary measures, if required.

11. Record keeping

Council will, at all times, maintain appropriate records of all data breaches, regardless of the seriousness of the data breach or whether it is immediately contained.

Data Breach Incident Register

Council will maintain an internal Data Breach Incident Register (which for practical purposes is combined with Council's Cybersecurity Incident Register) that details the following in relation to each eligible data breach:

- 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. That register will contain details of any data breaches for which Council was unable to directly notify individuals, or where it was not reasonably practicable to do so, and so the public were notified instead by the publication of a notice under section 59N(2) of the PPIP Act. The register will include a link to that public notification. 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.

12. Related Information

This policy will be included in the induction programs for all council officials.

See also:

- *Privacy Management Plan*
- *Cyber Security Incident Response Plan* (only accessible by council officers)
- *Cyber Crime and Security Incident Corporate Practice* (only accessible by council officers)

13. Review and testing

This policy will be tested and reviewed at least every 2 years.

14. Contact

- Manager Information Technology Ph 9911 9958
- Manager Governance & Risk Ph 9911 9910
- Director Corporate Services Ph 9911 9815