DATA BREACH POLICY P3.0239.3

www.camden.nsw.gov.au

DATA BREACH POLICY

DIRECTORATE: Customer and Corporate Strategy

BRANCH: Digital Technology & Innovation

CATEGORY: 3

1. Purpose

1.1 This Policy provides direction to Council staff in preparing for or responding to a data breach, especially involving personal or health information, with regard to the legislative framework.

1.2 This Policy must be read in conjunction with the Data Breach Response Procedure, the Privacy Management Plan and the Cyber Security Incident Response Plan.

2. Alignment with Community Strategic Plan

2.1 This Policy supports the following objective in Council's Community Strategy Plan (CSP):

- L3 – Our Council decisions are informed, accountable and transparent:
- L3.3 – Integrate long-term financial planning, safety, risk and strong governance across all Council operations.

3. Scope

3.1 This Policy applies to all data and information held by Council.

3.2 All Council officials must comply with this Policy in their conduct of official business for Council.

4. Objectives

4.1 The objectives of this Policy are to:

- Establish Council's commitment to meeting its obligations under the NSW Mandatory Notification of Data Breach (MNDB) Scheme.
- Provide the public with transparency over Council's approach to managing such breaches.

- Provide direction to Council staff in preparing for or responding to a data breach. Detailed procedures are provided in the Data Breach Response Procedure.

5. Policy Statement

5.1 Background

5.1.1 Amendments to the *Privacy and Personal Information Protection Act 1998* (PPIP Act) took effect on 28 November 2023. The amendments impact Council's responsibilities under the PPIP Act to notify affected individuals in the event of an eligible data breach of their personal or health information by Council.

5.2 Strategic Context

5.2.1 The PPIP Act provides for the protection of personal information and the privacy of individuals. Section 33 of the PPIP Act requires Council to prepare a Privacy Management Plan, outlining its policies and practices for compliance with the requirements of that Act and the *Health Records and Information Privacy Act 2002* (HRIP Act).

5.2.2 Under section 33(2)(c1) of the PPIP Act, the Privacy Management Plan must address the procedures and practices used by the agency to ensure compliance with the obligations and responsibilities set out in Part 6A of the MNDB Scheme. In doing so, it makes reference to this Policy.

5.2.3 The MNDB Scheme requires Council to notify the Privacy Commissioner and affected individuals about eligible data breaches. Council must prepare and publish a Data Breach Policy setting out how it will respond to a data breach.

5.3 Policy Requirements

5.3.1 Council publishes its Data Breach Policy to provide transparency and ensure accountability for the way it responds to data breaches.

5.3.2 Council establishes procedures to identify and prevent data breaches including technical controls, monitoring services, audits and reviews, as outlined in the Cyber Security Incident Response Plan.

5.3.3 Council maintains staff awareness of privacy and cyber security principles, current threat trends and provides training to identify, respond to and manage data breaches, as outlined in the Privacy Management Plan and the Cyber Security Incident Response Plan.

5.3.4 A member of the public or other external party can report a known or suspected data breach by phoning Camden on13 CAMDEN (13 226 336) or by sending an email to mail@camden.nsw.gov.au

5.3.5 A Council official must follow the Data Breach Response Procedure to report a known or suspected data breach as soon as possible and within 24 hours of the breach becoming known or suspected.

5.3.6 Council establishes procedures to manage a reported, known or suspected data breach, as detailed in the Data Breach Response Procedure, to:

- evaluate and triage breach reports;
- contain a breach and minimise any possible damage;
- assess the information involved and the associated risks, and implement appropriate actions to resolve and recover from the breach;
- notify affected individuals, the Privacy Commissioner and other organisations as required;
- review the incident and take action to prevent a recurrence.

5.3.7 In the event of an information security incident, Council will activate the Security Incident Response Team (SIRT) and appoint a Cyber Incident Response Manager to enable a coordinated response. The SIRT's responsibilities and escalation procedures are detailed in the Cyber Security Incident Response Plan.

5.3.8 The SIRT must immediately take all reasonable steps to contain a reported, known or suspected data breach and within 30 days,passess whether the incident falls within the scope of an eligible data breach.

5.3.9 If the breach cannot be assessed within 30 days, the Council must give written notice to the Privacy Commissioner regarding the extension period necessary to conduct the assessment.

5.3.10 The Cyber Incident Response Manager coordinates internal and external communications regarding information security incidents, with support from the Chief Information Officer and Manager Public Affairs. Key contacts are recorded in the Cyber Security Incident Response Plan.

5.3.11 Council maintains an internal register of all eligible data breaches which records the information specified under section 59ZE(2) of the PPIP Act.

5.3.12 Council maintains a public notification register in accordance with sections 59N(2) and 59P of the PPIP Act, to make information available when Council is unable to notify any or all of the individuals affected by an eligible data breach.

5.3.13 Council may need to notify or engage with other external stakeholders, suppliers or partners, depending on the circumstances of the data breach and the categories of information involved, as outlined in the Data Breach Response Procedure.

5.3.14 Council ensures that contracts, memorandums of understanding and agreements with external service providers (including other agencies) include controls to ensure compliance with privacy requirements and provisions in relation to the notification and remediation of data breaches.

5.3.15 Council maintains appropriate records to provide evidence of how suspected breaches are managed, including those not escalated to the SIRT or notified to the Privacy Commissioner. Recordkeeping requirements are described in the Cyber Security Incident Response Plan and aligned with the Records and Information Management Policy.

5.3.16 The Cyber Incident Response Manager provides support and advice to the Chief Information Officer on the implementation of this Policy, and written guidance to help staff meet their responsibilities.

5.4 Notification of Affected Parties

5.4.1 Council recognises that notification to individuals or organisations affected by a data breach can assist in mitigating any damage for those affected. Council will also consider the impact on individuals and the need to balance any harm or distress caused through notification against the potential harm that may result from the breach.

5.4.2 Council must notify individuals in the case of an eligible data breach, unless an exemption applies, and will consider notification in all cases of data breach.

5.4.3 Council will notify individuals or organisations affected by a data breach as soon as practicable. In some circumstances it may be appropriate to delay notification, for example where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

5.4.4 Council will notify affected individuals or organisations directly by telephone, letter, email or in person. Indirect notification, such as information posted on Council's website, a public notice in a newspaper,

or a media release, will only occur where the contact information of affected parties is 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).

5.4.5 The notification advice will be tailored to the circumstances of the particular breach. Content of a notification could include:

- information about the breach, including when it happened;
- a description of what data or personal information has been disclosed;
- assurances (as appropriate) about what data has not been disclosed;
- what Council is doing to control or reduce the harm;
- what steps the person or organisation can take to further protect themselves and what Council will do to assist people with this;
- Council's contact details for questions or requests for information; and
- the right to lodge a privacy complaint with the Privacy Commissioner.

6. Roles and Responsibilities

6.1. General Manager

6.1.1 The General Manager is responsible for ensuring compliance with the PPIP Act and HRIP Act, including Council's Privacy Management Plan and obligations under the MNDB Scheme.

6.2. All Council officials

6.2.1. All Council officials are responsible for ensuring their compliance with this Policy and the Data Breach Response Procedure.

7. Reporting

7.1. The Cyber Incident Response Manager monitors and reports on information security incidents and the management of data breaches against this Policy, to improve capability, efficiency and effectiveness.

8. Evaluation

8.1. The Chief Information Officer will annually review and ensure testing of systems and procedures that support this Policy.

8.2. Any failure to act in accordance with this Policy must be reported to the Chief Information Officer as soon as possible after the incident. If the act involves serious misconduct, it must be reported to the Chief Information Officer.

9. Definitions

Council	Camden Council.
Council official	Has the same meaning it has in the Model Code of Conduct for Local Councils in NSW and includes Councillors, members of staff of a Council, Administrators, Council Committee Members, and delegates of Council
Councillor	A person elected or appointed to civic office as a member of the governing body of Council who is not suspended, including the Mayor
Data breach	Any failure that causes or permits, or has the potential to cause or permit, unauthorised access, disclosure, modification, use or misuse of information held by Council. A data breach can occur within Council, between Council and another agency, or by a party external to Council.
Eligible data breach	An eligible data breach occurs when personal information (including health information) that is held by Council is accessed or disclosed without authorisation, or lost in circumstances that are likely to lead to unauthorised access or disclosure; and the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.
General Manager	The General Manager of Council and includes their delegate or authorised representative
Health information	Personal information that is information or an opinion about the physical or mental health or a disability of an individual; or an individual's express wishes about the future provision of health services to him or her; or a health service provided, or to be provided, to an individual; or genetic information that is or could be predictive of the health of an individual or their relatives or descendants; or other personal information collected in connection with the donation of human tissue.

Held	Council is in possession or control of the information; or the information is contained in a State record for which Council is responsible under the *State Records Act 1998*.
Information	Any data, document or message held by Council or staff.
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. This information can be on a database and does not necessarily have to be recorded in a material form.
Security Incident Response Team (SIRT)	The group of Council employees and resources responsible for responding to information security breaches – as established in the Cyber Security Incident Response Plan (Appendix 2).
Staff	Council employees (including full time or part time, permanent, temporary or casual), volunteers, consultants, contractors and their employees.
Suspected data breach	There are reasonable grounds to suspect there may have been an eligible data breach of Council.

10. Related Materials

10.1 Related Legislation

- *Health Records and Information Privacy Act 2002* (HRIP Act)
- *Privacy and Personal Information Protection Act 1998* (PPIP Act)

10.2 Related Policies, Procedures and Other Guidance Material

- Data Breach Response Procedure
- Privacy Management Plan

Approval and Review	
Responsible Branch	Digital Technology and Innovation
Responsible Manager	Director, Customer and Corporate Strategy
Date Adopted	Executive Leadership Group – 23/11/2023
Version	3
EDMS Reference	19/126467
Date of Next Review	Reviewed annually from date of adoption

Version Control

Version	Date Adopted	Approved By	EDMS Ref.	Description
1	21/02/2019	ELG	19/126467	Initial adoption of policy.
2	11/06/2020	ELG	19/126467	Minor Changes.
3	23/11/2023	ELG	19/126467	Amendments to include legislative requirements under the PPIP Act that come into effect 28 November 2023.

camden council

70 Central Ave,
Oran Park NSW 2570

13 CAMDEN (13 226336)

mail@camden.nsw.gov.au

PO Box 183, Camden 2570

camden.nsw.gov.au