CAMPBELLTOWN CITY COUNCIL	**POLICY**

Policy Title	Data Breach Policy
Related Documentation	Data Breach Action Plan Privacy Management Policy
Relevant Legislation	*Privacy and Personal Information Protection Act 1998* *Health Records and Information Privacy Act 2002*
Responsible Officer	Manager Governance & Risk

UNCONTROLLED WHEN PRINTED

Objective

1. The objective of this policy is to outline Campbelltown City Council's ("Council") protocol for the management of data breaches and to ensure Council's compliance with the Mandatory Notification of Data Breach ("MNDB") scheme.

Policy Statement

2. A data breach could have serious consequences for Council, creating risk through the disclosure of sensitive information which can impact the reputation, finances, interests or operations of Council.
3. Additionally, a data breach can damage Council's relationship with the community by creating a loss of trust and confidence in Council and the services we provide.
4. Responding quickly in the event of a data breach can substantially reduce the impact on any affected individuals and Council. Responding to a data breach includes determining if there has been an eligible data breach which is reportable under the MNDB scheme.

Scope

This policy applies to all Campbelltown City Council employees.

Definitions

Term	Definition
Data Breach	For the purposes of this policy, a data breach is the unauthorised access to, or disclosure of, or loss of personal and health information held by Council.
Unauthorised Access	For the purposes of this policy, unauthorised access is the access of personal and health information held by Campbelltown City Council by a person or persons without appropriate delegation or authority to do so.
Campbelltown City Council Employee (Council Employee)	Includes full time, part time, casual, temporary and fixed term employees, agency staff and contractors. For the purpose of this policy, employees also include volunteers, trainees and students on work placements.

Personal Information	Information or an opinion of an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Health Information	Information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Legislative Context

1. Part 6A of the *Privacy and Personal Information Protection Act 1998* ("PPIP Act") establishes the NSW Mandatory Notification of Data Breach scheme.
   (a) The MNDB scheme requires that, in the event of a data breach, Council must notify the Privacy Commissioner and affected individuals of eligible data breaches.
   (b) The MNDB scheme requires Council to prepare and publish a Data Breach Policy for managing such data breaches.

Principles

2. The MNDB scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be determined from the information or opinion.
3. The MNDB does not apply to data breaches that do not involve personal information or health information, or to breaches that not likely to result in serious harm to an individual. Where the scheme does not apply, Council is not required to notify individuals or the Commissioner but should still take action to respond to the breach.
4. Council holds obligations under the NSW MNDB scheme reporting to the NSW Privacy Commissioner.
   (a) In some cases, Council may be subject to the Commonwealth Notifiable Data Breach ("NDB") scheme which is reportable to the Office of the Australian Information Commissioner ("OAIC").
   (b) An example would be where a data breach involves federal data such as Tax File Numbers and the breach is likely to result in serious harm then the breach would be reportable to the OAIC as well as to the NSW Privacy Commissioner.

What is an Eligible Data Breach?

5. An eligible data breach occurs where:
   (a) there is unauthorised access to, or unauthorised disclosure of, personal information held by Council, and a reasonable person would determine that the access and/or disclosure of the information would likely result in serious harm to a person to whom the information relates, or,
   (b) personal information held by Council is lost in circumstances where:
      i. unauthorised access to and/or unauthorised disclosure of the information is likely to occur, and
      ii. a reasonable person would determine that the access and/or disclosure of the information would likely result in serious harm to a person to whom the information relates.
6. An eligible data breach may include a breach:
   (a) within Council,
   (b) between Council and other government agencies,
   (c) that occurs by an external person or entity accessing data held by Council without authorisation.

7. Examples of a data breach include:
   (a) Cyber incident such as ransomware, malware, hacking, phishing or brute force access attempts result in access to or theft of personal information.
   (b) A device with personal information is lost or stolen.
   (c) Personal information is mailed or emailed to the wrong person.
   (d) Hardcopy records with personal information is left in a discarded cabinet.

Data Breach Management Framework

8. Each data breach that may occur will be assessed on a case-by-case basis and no template response can be applied to all instances where there may be a data breach.
9. Rather Council will implement a Data Breach Management Framework intended to guide Council employees on the actions that should be taken in the event of a data breach.
10. A Data Breach Management Framework includes the implementation of a:
    (a) Data Breach Response Team, and
    (b) Data Breach Response Plan.

Data Breach Response Team

11. In the event of a data breach, Council will appoint a data breach response team. The team will be responsible for managing the data breach.
12. The Council employees appointed to the Data Breach Response Team will be determined on a case-by-case basis depending on the nature of the breach and where the breach occurred.
13. A Data Breach Response Team will include:
    (a) Council's Privacy Officer.
    (b) The team leader or coordinator of the team from where the breach originated.
    (c) Manager / Executive Manager, of the section from where the breach originated.
    (d) In the event of a Cyber incident, the Executive Manager of Corporate Support & Systems.

Data Breach Response Plan

14. In the event of a data breach, Council will follow the key action principles of the Data Breach Response Plan, these are:
    (a) Contain and Report
    (b) Assess
    (c) Notify
    (d) Review
    (e) Document and Record

Key Action Principles

15. Contain and Report:

(a) Should a Council employee become aware of a breach, they should consider if there are any immediate actions that can be taken to contain the breach.

i. Examples of immediate actions include:

1. If information has accidently been emailed to the wrong person, are you able to recall the email, or contact the recipient and ask them to not open the email and delete the information.
2. If you have misplaced a Council issue mobile phone, contact IT immediately to see if the phone can be remotely locked and logged out of any Council applications.

(b) The event must be reported as soon as possible to the Council employee's direct report, for example, their Team Leader, Coordinator, Manager, or Executive Manager.

i. For the purposes of this Data Breach Response Plan the report of the breach must be made within an hour of the breach having been identified.

(c) The event must be reported to Council's Privacy Officer. The report needs to specify the type of the breach, the type of information that has been compromised and any immediate actions taken to contain the breach and if these actions were successful.

i. For the purposes of this Data Breach Response Plan, Council's Privacy Officer must be notified of the breach on the day that the breach has been identified.

(d) Should the breach be successfully contained, the breach must still be reported to Council's Privacy Officer for the incident to be recorded on Council's Privacy Breach Incident Register. Additionally, a review of the incident will need to be undertaken, (see point 18 below).

16. Assess:

(a) Councils Privacy Officer will assess the data that has been compromised and determine if the incident is an eligible data breach.

i. Factors to be considered are:

1. Type of personal information that was compromised.
2. Sensitivity of the information.
3. Whether the information is protected by security measures.
4. Who could have obtained the information.
5. The harm that may occur in the disclosure of this information.
6. Any other factors and guidelines provided by the NSW Information and Privacy Commissioner.

ii. The assessment of the data breach must be completed within 30 days of the breach occurring. If the Privacy Officer is satisfied that the assessment cannot be reasonably completed within the 30 days, an extension of time may be approved.

(b) In the event that the Privacy Officer has deemed the incident to be an eligible data breach, appropriate consultation may be undertaken with the Communications Team.

17. Notify:

(a) If it is determined that an eligible data breach has occurred, then Council must notify the:

i. NSW Privacy Commissioner immediately, and

ii. Individuals affected by the data breach as soon as reasonably practicable.

iii. In the event that the data breach includes information that would affect a Federal Government agency, Council may also be required to notify the Australian Privacy Commissioner, (see point 24 below).

(b) Council's Privacy Officer is responsible for notifying the NSW Privacy Commissioner.

(c) The team/section/division of Council, where the data breach originated will be responsible for notifying individuals affected by the data breach. Council's Privacy Officer will liaise with the team and provide guidance and support in executing the notification process.

18. Review:

(a) Preventing any future data breaches is of the highest priority to Council. As such, in the event of a data breach occurring a key component of the Data Breach Response Plan is to review the incident and determine if there are any steps that can be taken to prevent a similar occurrence.

(b) The team/section/division of Council where the data breach occurred will need to undertake a review of the incident and consider any appropriate measures that should be taken.

(c) The review should consider the following:

i. What went wrong?

ii. Are there any processes and or procedures that could be improved to prevent this happening again?

iii. Is there a gap in knowledge that would need to be rectified with relevant training?

(d) Council's Privacy Officer must be notified of the outcome of the review.

19. Document and record:

(a) All records, information and documents related to the privacy breach, it's investigation and outcome must be recorded.

(b) Council's Privacy Officer will create an Incident file in Council's Electronic Document and Records Management System, IRIS.

(c) All internal emails, reports notes, investigations and outcome materials must be uploaded to the relevant file in IRIS. All Council employees hold a responsibility to document their involvement appropriately and accurately.

(d) All incidents must be recorded in Council's Data Breach Incident Register.

(e) All eligible data breaches must be recorded in Council's Eligible Data Breach Notification Register which must be published on Council's website.

Effectiveness of this Policy

20. This policy will be reviewed in accordance with Council's Corporate Document Review Framework contained within the Corporate Documents Authorised Statement

21. In accordance with the NSW Information and Privacy Commission recommendations the Data Breach Response Plan will be reviewed, tested, and updated annually.

END OF POLICY STATEMENT