Central Coast Council

Data Breach Policy

Date Adopted: **26/04/2024**
Revision: **3**
Policy No.: **CCC047**

Table of Contents

1. Policy Objectives

1.1. The objectives of this Policy (and the associated *Data Breach Procedure* (**Procedure**)) are to:

1.1.1. outline how Central Coast Council (**Council**) will identify, assess, manage, and respond to data breaches, particularly those involving personal information in accordance with the requirements of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**).

1.1.2. provide detail about:

a) what constitutes an eligible data breach under the PPIP Act;

b) the roles and responsibilities within Council for reporting, reviewing and managing data breaches; and

c) the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

1.1.3. ensure Council's compliance with the PPIP Act, the *Health Records and Information Privacy Act 2002* (**HRIP Act**) and the *Privacy Act 1988* (Cth) (**Privacy Act**) as governed by the Office of the Australian Information Commissioner (**OAIC**) and NSW Information and Privacy Commission (**IPC**), regarding handling personal and health information.

---

2. Policy Scope

2.1. This Policy applies to all staff and contractors of Council, including Councillors, students, volunteers, agency personnel and third-party providers who hold personal and health information on behalf of Council.

2.2. This Policy includes Council data held in any format (paper based or electronic) however, it does not apply to information that has been classified as public.

2.3. Depending on the type and extent of the data breach, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities. These activities are outside the scope of this Policy, which is limited to the immediate internal responses of business units.

---

3. Policy Statement

3.1. Council is committed to ensuring, as far as practicable, that the data it holds is secure from potential data breaches and will regularly review, develop, maintain and test its systems and procedures to support data security and this Policy.

3.2. Having a data breach response plan and policy is part of establishing robust and effective privacy and information governance procedures. Effective breach management assists Council in avoiding or reducing possible harm to both the

affected individuals/organisations and Council and may prevent future breaches.

3.3. To support Council's obligations under the PPIP Act, and to promote robust and effective privacy, data handling and information governance procedure, Council also has a Data Breach Procedure. The Procedure outlines the steps for managing a data breach, including providing examples of situations that will be considered an eligible data breach, the steps involved in responding to a data breach, and the considerations around notifying persons whose privacy may be affected by the breach.

3.4. This Policy should be read in conjunction with Council's Privacy Management Plan Policy which provides more information on how Council may collect, use, and disclose personal information and the Data Breach Procedures.

4. What is an eligible data breach?

4.1. A data breach occurs when personal information held by Council (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

4.2. Under the Notifiable Data Breaches (**NDB**) Scheme, any organisation or agency covered by the Privacy Act must notify individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

4.3. For Council, it is mandatory to apply the NDB Scheme to tax file numbers it holds.

4.4. This may or may not involve disclosure of personal information external to Council or publicly. For example, unauthorised access to personal information by a Council employee, or unauthorised sharing of personal information between teams within Council may amount to a data breach.

4.5. A data breach may occur as the result of malicious action, system failure or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (**IPPs**).

4.6. Examples include:

Human error

4.6.1. When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.

4.6.2. When system access is incorrectly granted to someone without appropriate authorisation.

4.6.3. When staff fail to implement appropriate password security, for example, not securing passwords or sharing password and login details.

4.6.4. When a letter or document is posted to an incorrect address; or an email is sent to an incorrect recipient; or information is published on Council's website without consent.

System failure

4.6.5. When a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.

4.6.6. Where systems are not maintained through the application of known and supported patches.

Malicious or criminal attack

4.6.7. Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.

4.6.8. Social engineering or impersonation leading to inappropriate disclosure of personal information.

4.6.9. Insider threats from Council employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

4.6.10. Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

4.7. The MNDB Scheme applies where an eligible data breach has occurred. For a data breach to constitute an eligible data breach under the MNDB Scheme, there are two tests to be satisfied:

4.7.1. 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

4.7.2. 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.

Meaning of 'serious harm'

4.8. The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as a result of a data breach are context-specific and will vary based on:

4.8.1. The type of personal information accessed, disclosed or lost, and whether a combination of different types of personal information might lead to increased risk;

4.8.2. The level of sensitivity of the personal information accessed, disclosed or lost;

4.8.3. The amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach;

4.8.4. The circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm);

4.8.5. The circumstances in which the breach occurred; and

4.8.6. Actions taken by Council to reduce the risk of harm following the breach.

4.9. Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

4.10. Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the data breach.

5. Systems and processes for managing data breaches

5.1. Council has established and implemented a comprehensive set of controls, measures and processes for preventing, responding to and managing data breaches.

5.2. This includes projects to increase cyber security maturity, cyber security training for all staff, robust access controls, data encryption, network and endpoint security measures, data loss prevention systems and incident response plans.

5.3. An up-to-date inventory of assets is maintained, and 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.

5.4. Council will ensure all third-party providers who store personal and health information on behalf of Council are aware of the MNDB Scheme and the obligations under this Policy to report any eligible data breaches to the IPC.

5.5. Council also has a range of policies and procedures to prevent, control and mitigate exposures to breaches of data, including its Code of Conduct, Privacy Management Plan Policy and Fraud and Corruption Control Framework.

5.6. To mitigate the risk of data breaches, Council regularly conducts training to educate employees about the risks associated with data breaches, and their

responsibilities as a public official to recognise, respond, report and prevent such incidents.

5.7. Council also maintains an internal register for data breaches and has implemented recommended changes to systems and policies in response to reviewing the causes of data breaches to assist in preventing future breaches.

6. Responding to a data breach

6.1. Each data breach is unique and will require a tailored response. The response actions will depend on several factors, including the type of data compromised, the cause of the breach and the potential harms that could arise for affected individuals.

6.2. While the details of each breach will be different, the process for responding to a data breach is the same and will be followed in each instance to ensure a consistent approach.

6.3. In line with the recommendations from the IPC, Council will follow the below steps when investigating and responding to a data breach:

6.3.1. Initial report and triage;

6.3.2. Contain the breach;

6.3.3. Assess and mitigate;

6.3.4. Notify; and

6.3.5. Review.

6.4. The full procedure for investigation of a data breach is set out in the *Data Breach Procedure*.

7. Responsibilities

Compliance, monitoring and review

7.1. The following staff have identified roles under this Policy:

Privacy Contact Officer

7.1.1. The Privacy Contact Officer is responsible for implementing this Policy, reporting data breaches to the Chief Executive Officer and all notifications and actions for eligible data breaches.

Chief Executive Officer (or their delegate)

7.1.2. The Chief Executive Officer (or their delegate) is responsible for notifying the Privacy Commissioner after an eligible data breach is identified.

7.1.3. The Chief Executive Officer (or their delegate) will determine the method and oversee the notification of any affected individuals of a

data breach, including eligible data breaches under the MNDB Scheme.

Section Manager Governance

7.1.4. The Section Manager Governance is responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches.

7.1.5. The Section Manager Governance will provide advice on the communication strategy and messaging to affected individuals and external reporting agencies.

Governance Team

7.1.6. The Governance Team is responsible for monitoring and reviewing the type of data breaches (including those under the MNDB Scheme) to identify trends and areas of concern where staff may require additional training and systems and processes need to be remediated to prevent future incidents.

7.1.7. The Governance Team is responsible for preparing an annual report to Council's Executive Leadership Team on the number and nature of data breach incidents within Council.

All Council Employees

7.1.8. All employees have a responsibility for immediately reporting a suspected data breach in accordance with this Policy and the Procedure.

7.2. This Policy will be reviewed, tested, and updated in accordance with Council's Policy Framework or as required by best practice or legislation.

7.3. Suspected breaches or misuse of this policy are to be reported to the Chief Executive Officer. Alleged breaches of this policy shall be dealt with by the processes outlined for breaches of the *Code of Conduct*, as detailed in the *Code of Conduct* and in the *Procedures for the Administration of the Code of Conduct*.

Reporting

7.4. Council will report all eligible data breaches in accordance with the MNDB Scheme and the PPIP Act.

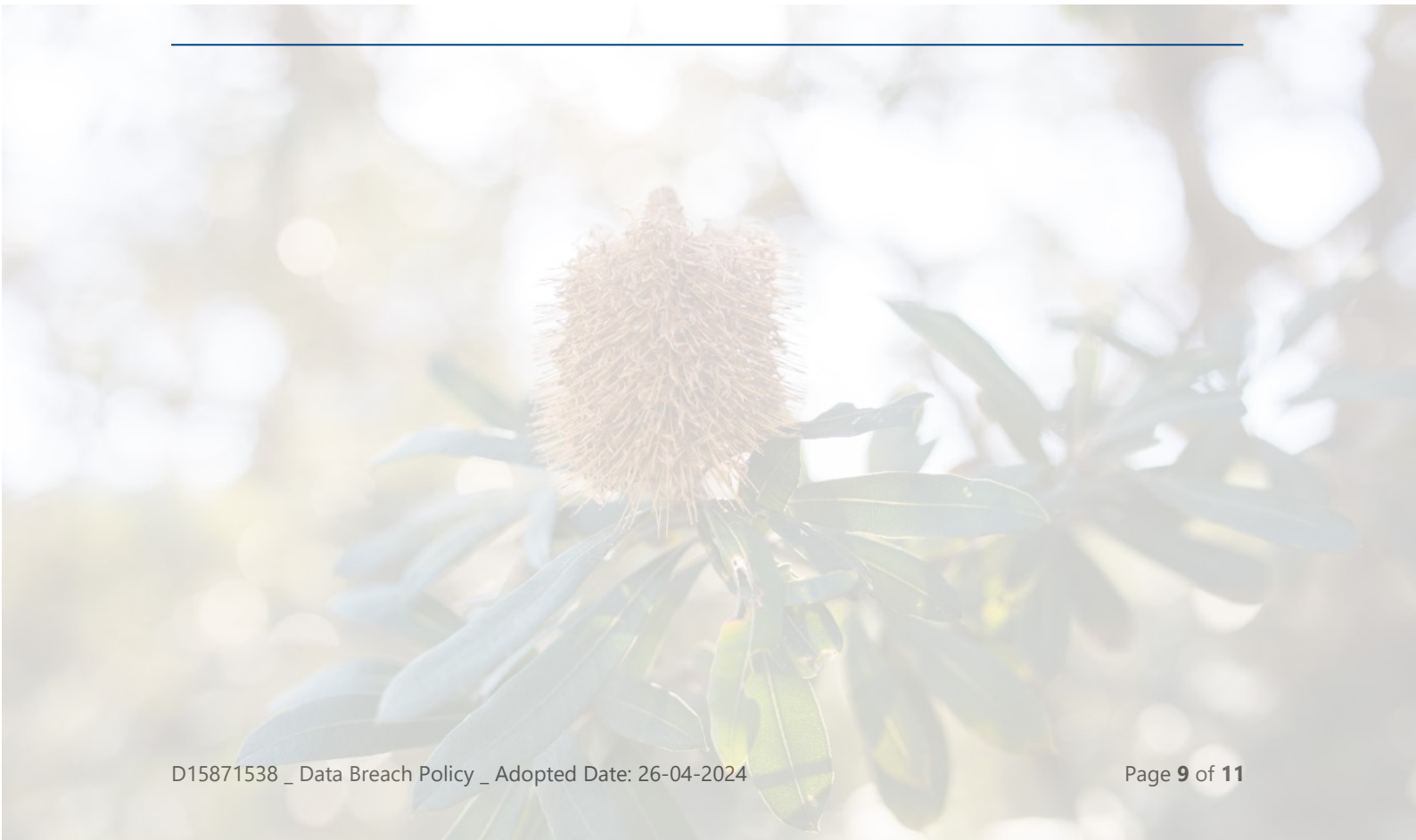
7.5. An annual report will be provided to Council's Executive Leadership Team outlining the number and nature of data breach incidents within Council. This report may also be provided to Council's Audit, Risk and Improvement Committee where appropriate.

Records management

7.6. Staff must maintain all records relevant to administering this Policy in accordance with Council's Information and Records Management Policy.

8. Policy Definitions

Act	means the *Local Government Act 1993* (NSW)
Affected individual	means an *affected individual* as defined in the PPIP Act.
Council	means Central Coast Council
Council Officer	means any officer or employee of Council.
Data Breach	means the unauthorised access to, or inadvertent disclosure, access, modification, use, misuse or loss of, or interference with Personal Information held by Council and in this Policy includes a potential Data Breach.
Personal Information	for the purposes of the MNDB Scheme means '*information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion*.' This also includes information about an individual's physical or mental health, disability and information connected to the provision of a health service.
Relevant Manager or Director	means the manager or Director to whom a Council Officer responsible for the data subject to the breach reports or Director with responsibility for a contract with a third party.
Staff	means Council's permanent, temporary or casual employees, volunteers, and contractors.



9. Policy Administration

Business Group	Corporate Services
Responsible Officer	Privacy Contact Officer/Unit Manager Governance Risk and Legal
Associated Procedure (if any, reference document(s) number(s))	Data Breach Procedure (D15871576)
Policy Review Date	Four years from date of adoption unless legislated otherwise
File Number / Document Number	D15871538
Relevant Legislation (reference specific sections)	This Policy supports Council's compliance with the following legislation: ▪ *Data Sharing (Government Sector) Act 2015* ▪ *Health Records and Information Privacy Act 2002* ▪ *Privacy Act 1998 (Cth)* ▪ *Privacy and Personal Information Protection Act 1998* ▪ *State Records Act 1998*
Link to Community Strategic Plan	Theme 4: Responsible **Goal G: Good governance and great partnerships** R-G3: Provide leadership that is transparent and accountable, makes decisions in the best interest of the community, ensures Council is financially sustainable and adheres to a strong audit process.
Related Policies / Protocols / Procedures / Documents (reference document numbers)	▪ Information and Records Management Policy ▪ Code of Conduct ▪ Delegations Register

10. Policy Authorisations

No.	Authorised Function	Authorised Business Unit / Role(s)
	Determine an eligible Data Breach.	Privacy Contact Officer (or their delegate)
	Notify the individual, OAIC and IPC of an eligible data breach.	Privacy Contact Officer (or their delegate)

11. Policy History

Revision	Date Approved / Authority	Description Of Changes
1	22 June 2020 D14036850	New policy adopted to protect the privacy and personal information of Council's customers, staff, consultants, elected representatives and the security of its data
2	24 June 2021 D14703147	Review to amend position titles as a result of the organisational restructure and to amend policy review period to 3 years
3	12 December 2023 Minute No. 229/23 (public exhibition) 26 March 2024 Minute No. 74/24 (adoption)	Major review to reflect changes to the *Privacy and Personal Information Act 1998* and the introduction of the Mandatory Notification of Data Breach Scheme