Central Coast Council

Data Breach Procedure

Date Adopted: **28/11/2023**
Revision: **3**
Policy No.: **CCC0047**

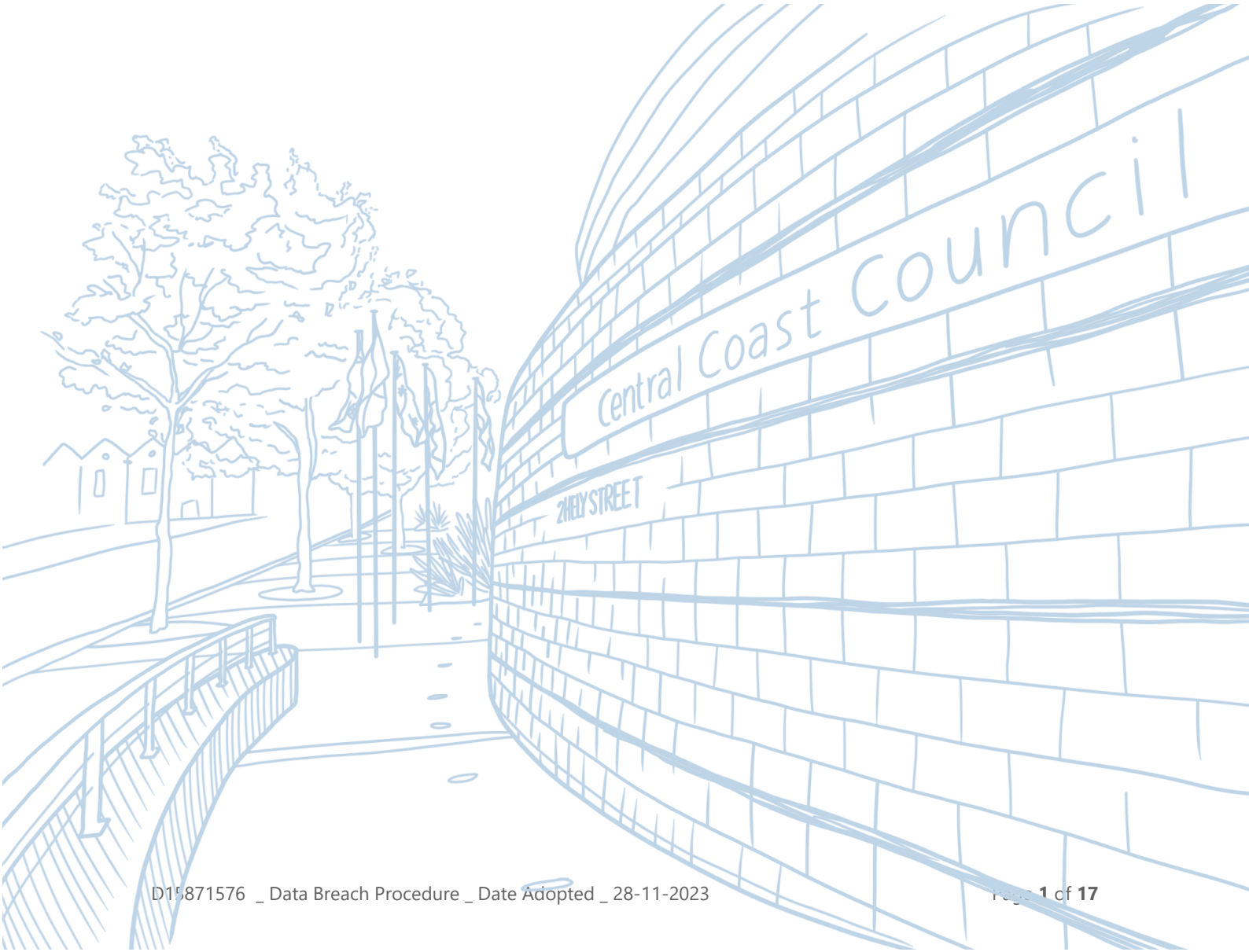


Table of Contents

1. Procedure Purpose

1.1. The object of this Procedure is provide guidance and steps for staff to follow when responding to a breach of Central Coast Council (**Council**) held data.

---

2. Procedure Scope

2.1. This Procedure applies to:

2.1.1. 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.

2.1.2. Council data held in any format (paper based or electronic). The Procedure does not apply to information that has been classified as public.

---

3. Procedure Statement

3.1. Council is committed to ensuring, as far as practicable, that the data it holds is secure from potential data breaches. Where a breach of that data does occur, it is essential that there are appropriate steps in place to ensure quick and appropriate action is taken.

3.2. Having a data breach response plan, policy and procedure is part of Council's privacy and information governance procedures and framework. Effective breach management assists Council in avoiding or reducing possible harm to both affected individuals or organisations and Council and may prevent future breaches.

3.3. This Procedure 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 as well as the Data Breach Policy.

---

4. Reporting and responding to a data breach

4.1. Council's response to a data breach will be undertaken promptly to enable Council to contain, assess and respond to data breaches efficiently, as well as to help minimise harm to affected individuals.

4.2. There are five key steps required in responding to a data breach or suspected data breach:

4.2.1. Initial report and triage;

4.2.2. Contain the breach;

4.2.3. Assess and mitigate;

4.2.4. Notify; and

4.2.5. Review.

4.3. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

4.4. The Privacy Contact Officer must be informed of any data breach or suspected data breach to ensure Council meets its legislative obligations, including notifying the Privacy Commissioner for eligible data breaches and affected individuals and the Office of the Australian Information Commissioner (**OAIC**) as required.

4.5. Where appropriate, the Section Manager Governance will ensure that appropriate advice and information is provided to relevant Council staff to assist in responding to any enquiries made by the public, preparing appropriate communications and managing complaints that may be received as a result of the data breach.

4.6. Each step is set out in further detail below.

Step 1: Initial report and triage

4.6.1. Any staff member, contractor or third-party provider who becomes aware of a data breach or becomes aware that are grounds to suspect a data breach is to notify the Privacy Contact Officer or the Governance Team immediately and provide details of the breach.

4.6.2. The Privacy Contact Officer or their delegate will review the information provided and notify the Chief Executive Officer (or their delegate) of any eligible data breach.

4.6.3. Council may also convene a Data Breach Response Team where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual.

Step 2: Contain the breach

4.6.4. Containment of the breach is prioritised by Council and all necessary steps possible must be taken to contain the breach and minimising any resulting damage. This obligation is ongoing as the other steps proceed.

4.6.5. Examples of containment methods may include:

a) Stop any unauthorised practice(s) and suspend the activity that led to the breach;

b) Recover any records or personal information;

c) Shut down the system that was breached (if practicable); and/or

d) Revoke or change the account privileges or change access codes or passwords.

4.6.6. If a third party is in possession of the data and refuses to return it, it may be necessary for Council to seek legal or other advice on what action can be taken to recover the data.

4.6.7. When recovering data, Council will make sure that copies that have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third party that the copy of the data that they received in error has been permanently deleted.

Step 3: Assess and mitigate

4.6.8. Council will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme and the risks and potential for serious harm associated with the breach.

4.6.9. The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. The Section Manager Governance will prepare a report and provide to the Privacy Contact Officer who will review the proposed actions and recommendations of the report prior to the Report being provided to the Chief Executive Officer for approval.

4.6.10. Data Breach Report and Action Plans are to be saved in in the appropriate folder in Council's electronic record keeping system. (F2022/02634).

4.6.11. The Privacy Contact Officer will be responsible for the implementation of proposed actions and recommendations.

4.6.12. After a suspected data breach is reported to the Chief Executive Officer or their delegate, an assessment must be carried out within 30 days to determine whether there are reasonable grounds to believe that the suspected data breach is an eligible data breach. This date may be subject to an extension in accordance with the PPIP Act.

4.6.13. A thorough evaluation of the risks will assist Council in determining the appropriate course of action to take. The factors that may be considered (but are not limited to) when assessing the breach include:

a) The type of information is involved in the breach

b) The sensitivity of the personal information involved in the breach;

c) Whether the personal information is or was protected by security measures;

d) The persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given,

e) The likelihood of the persons who has received or has access to the personal information has or had the intention of causing harm or could or did circumvent security measures protecting the information;

f) The nature of the harm that has or may occur; and

g) Other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

4.6.14. Further actions may include interviews (or further interviews) with staff involved and/or affected, or the request of further investigation by appropriate Council staff into system failures or IM&T security issues.

4.6.15. During the assessment, the Chief Executive Officer must make all reasonable attempts to mitigate the harm done by the suspected breach.

4.6.16. To mitigate the breach, Council will consider the following measures:

a) Implementation of additional security measures within Council's own systems and processes to limit the potential for misuse of compromised information.

b) Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites.

c) Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution to advise caution when relying on particular identity documents for particular cohorts.

Step 4: Notify

4.6.17. If an eligible data breach has occurred, the notification process under the MNDB Scheme is triggered. There are four elements of the notification process:

a) The Chief Executive Officer (or their delegate) will **immediately** notify the Privacy Commissioner after an eligible data breach is

identified using the approved form as published on the IPC's website.

b) Determine whether an exemption to notification applies. If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, Council may not be required to notify affected individuals.

c) If an exemption does not apply, notify affected individuals or their authorised representatives **as soon as practicable**; and.

d) Provide any further information to the Privacy Commissioner.

4.6.18. The Chief Executive Officer (or their delegate) and the Response Team (if appointed) will determine how to notify, and oversee the notification to, affected individuals of the eligible data breach in accordance with this Procedure and the PPIP Act.

4.6.19. If a data breach is not an eligible data breach under the MNDB Scheme, Council may still consider notifying individuals/organisations of the breach, dependent on the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual/organisation to take further steps to avoid or remedy harm.

4.6.20. The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

4.6.21. Considerations include the following:

When to notify

4.6.22. Individuals/organisations affected by a data breach will be notified as soon as reasonably practicable. While this Procedure sets a target of 5 days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, Council will consider issuing a public notification on its website.

How to notify

4.6.23. Notification should be direct either by phone, letter, email or in person, to the affected individuals/organisations.

4.6.24. Indirect notification, such as information posted on Council's website, posted notices or media releases should only occur where direct notification could cause further harm, is cost prohibitive or the contact information for affected individuals/organisations is unknown. The Chief Executive Officer can also determine to issue a public notification if it is appropriate.

4.6.25. A record of any public notification of a data breach will be published on Council's website and recorded on the Public Data Breach Register for a period of 12 months.

What to say

4.6.26. The following information must, if reasonably practicable, be included in a notification to an affected individual of a data breach:

a) The date the breach occurred;

b) A description of the breach;

c) How the breach occurred;

d) The type of breach that occurred;

e) The personal information included in the breach;

f) The amount of time the personal information was disclosed for;

g) Actions that have been taken or are planned to secure the information, or to control and mitigate the harm;

h) Recommendations about the steps an individual should take in response to the breach;

i) Information about complaints and reviews of agency conduct;

j) The name of the agency or agencies that were subject to the breach;

4.6.27. Contact details for the agency subject to the breach or the nominated person to contact about the breach.

Other obligations including external engagement or reporting

4.6.28. Council will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner) where a data breach occurs.

4.6.29. Depending on the circumstances of a data breach, such as an intentional or suspected serious data breach and the categories of data involved, it may be appropriate to notify other agencies/third parties, such as:

a) The OAIC, where a data breach may involve agencies under Federal jurisdiction;

b) The NSW Police Force and/or Australian Federal Police, where Council suspects a data breach is a result of criminal activity;

c) Cyber Security NSW, where a data breach is a result of a cyber security incident;

d) The Australian Cyber Security Centre, where a data breach involves malicious activity from a person or organisation based outside Australia;

e) Council's insurance providers;

f) Credit card companies, financial institutions/services providers;

g) Professional associations, regulatory bodies or insurers, where a data breach involves malicious activity from a person or organisation outside Australia; and/or

h) Other internal or external parties who have not already been notified.

4.6.30. Any reported incidents of suspected misconduct must also be reported to Council's Disclosures and Investigations Coordinator as soon as practicable.

4.6.31. Where a data breach is subject to the NDB Scheme (which for Council is currently limited with respect to tax files numbers), Council must promptly notify individuals at likely risk of serious harm as well as the OAIC. The notification must include:

a) Information identifying Council and its contact details;

b) A description of the data breach;

c) The kinds of information concerned; and

d) Recommendations about the steps that individuals should take in response to the data breach.

4.6.32. The Chief Executive Officer (or their delegate) and the Response Team (if appointed) will determine how to notify and oversee the notification made to the OAIC and any affected individuals of the NDB Scheme data breach.

4.6.33. Council may become subject to other legislation relevant to data breaches impacting on other agencies. For example, under the *Data Sharing (Government Sector) Act 2015*:

a) If Council is the recipient of data from another NSW Government agency that contains personal information or health information, and

b) Council becomes aware that the Privacy and Personal Information Protection Act 1998 or the Health Records and Information Privacy Act 2002 has been or is likely to be

contravened in relation to that information while in Council's control

4.6.34. In such instances, Council must inform the other agency and the NSW Privacy Commissioner of the contravention as soon as practicable after becoming aware of it.

Step 5: Review

4.6.35. Council must ensure that the cause of the breach has been fully investigated, and that the appropriate people have been briefed on outcomes and recommendations. This includes investigating the circumstances of data breaches to determine all relevant causes and consider what short or long-term measures can be taken to prevent any reoccurrence.

4.6.36. Depending on the nature of the breach, this step may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step 3 above.

4.6.37. Preventative actions could include:

a) Review of Council's IT systems and remedial actions to prevent future data breaches;

b) Security audit of both physical and technical security controls

c) Review of policies and procedures

d) Review of staff/contractor training practices

e) Review of contractual obligations with contracted service providers.

4.6.38. At a minimum, amendments to relevant policies and procedures should be made where necessary, and staff training should be undertaken where deemed appropriate.

4.6.39. A debriefing session should be held with relevant staff to assess the cause of and response to the breach, and to ensure any necessary recommendations are allocated and actioned appropriately.

4.6.40. Any recommendations to implement the above preventative actions are to be approved by the Chief Executive Officer and documented in Council's electronic record keeping system.

4.6.41. Consideration will be given to reporting relevant matters to Council's Audit, Risk and Improvement Committee and to Council.

Data Retention

4.6.42. When a data breach incident is being investigated, all records are to be documented and recorded in Council's electronic record keeping

system, including all related documents and supporting evidence of a breach.

5. Responsibilities

Compliance, monitoring and review

5.1. The following staff have identified roles under this Procedure:

Privacy Contact Officer

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

Chief Executive Officer (or their delegate)

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

5.1.3. 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

5.1.4. 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.

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

Governance Team

5.1.6. 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.

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

All Council Employees

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

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

Reporting

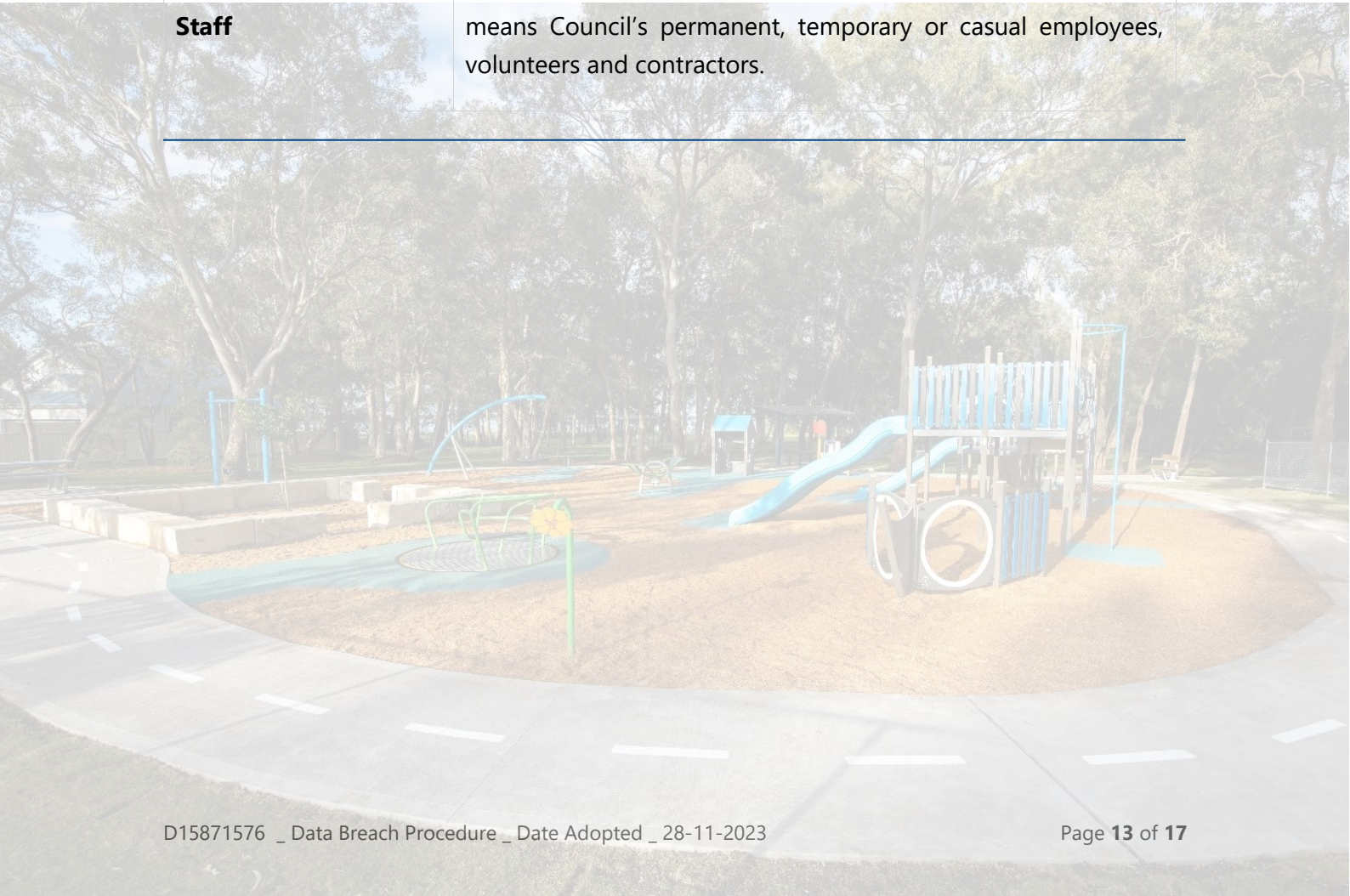
5.3. Council will report all eligible data breaches in accordance with the MNDB Scheme and the *Privacy and Personal Information Protection Act 1998* (PPIP Act). An annual report will be provided Council's Executive Leadership Team outlining the number and nature of data breach incidents within Council. This report may also be provided to Council's Audit, Risk and Improvement Committee where appropriate.

Records management

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

6. Procedure 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
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 Procedure, 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.



7. Procedure Administration

Business Group	Corporate Services
Responsible Officer	Privacy Contact Officer/Unit Manager Governance Risk and Legal
Associated Policy (if any, reference document(s) number(s))	Data Breach Policy (D15871538)
Procedure Review Date	Four years from date of adoption unless legislated otherwise
File Number / Document Number	D15871576
Relevant Legislation (reference specific sections)	This Procedure supports Council's compliance with the following legislation: ▪ *Data Sharing (Government Sector) Act 2015* ▪ *Health Records and Information Privacy Act 2002* ▪ *Privacy Act 1988* (Cth) ▪ *Privacy and Personal Information Protection Act 1998* ▪ *State Records Act 1998*
Relevant desired outcome or objectives as per Council's Delivery Program	Theme 4: Responsible **Goal G: Good governance and great partnerships** R-G2: Engage and communicate openly and honestly with the community to build a relationship based on trust, transparency, respect and use community participation and feedback to inform decision making.
Related Policies / Protocols / Procedures / Documents (reference document numbers)	▪ Information and Records Management Policy ▪ Code of Conduct ▪ Delegations Register

8. Procedure 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)

9. Procedure History

Revision	Date Approved / Authority	Description Of Changes
1	22 June 2020	New procedure adopted
2	24 June 2021	Review to amend Position Titles as a result of the organisation restructure.
3	28 November 2023 ELT Minute No. 1.5	Major review to reflect the changes to the *Privacy and Personal Information Protection Act 1998* and the introduction of the MNDB Scheme and refining procedures to reflect current Council practices.

10. Appendices

Appendix 1: Data Breach Report and Action Plan

Appendix 1: Data Breach Report and Action Plan

Data Breach Report and Action

Description of Data Breach	When?	
	What?	
	How?	
Action taken	Notification	
	Containment	
Description of risks	Risk?	
	Harm?	
	Affecting?	
Description of causes	How?	
	Why?	
	Is this a systemic issue?	
Action Proposed	Change?	
	Train?	
	Remind?	
	Stop?	
	Media?	
	Remedy?	
	Other matters?	

Notification to Privacy Commissioner?	

Data Breach Handling Officer		**Action**		Date	
Privacy Contact Officer		**Action**		Date	
Chief Executive Officer		**Action**		Date	