Data Breach **Policy**

June 2021

Policy No: CCC 047

Policy owner:	Governance and Business Services, Governance
Approved by:	David Farmer, Chief Executive Officer
Date of approval:	24 June 2021
Policy category:	Operational
Content Manager No:	D14036854
Review date:	June 2024

Central Coast Council P: 1300 463 954 E: ask@centralcoast.nsw.gov.au W: centralcoast.nsw.gov.au
A: Wyong: 2 Hely St / PO Box 20, Wyong NSW 2259 Gosford: 49 Mann St / PO Box 21, Gosford NSW 2250

Contents

Purpose

1. To protect important business assets (data) including personal information and Council's reputation.

2. To support Council's legal obligations under the NSW *Privacy and Personal Information Protection Act 1998*, *Health Records and Information Privacy Act 2002* and requirements governed by the Federal Office of the Australian Information Commissioner (OAIC) and the NSW Information and Privacy Commission (IPC) with respect to handling personal and health information.

3. To ensure effective breach management, including notification where warranted, assists the Council in avoiding or reducing possible harm to both the affected individuals/organisations and the Council, and may prevent future breaches.

4. To detail the principles, goals and responsibilities associated with the mandatory data breach notification and data response planning.

Policy summary

5. This policy outlines Council's commitment to protect the privacy and personal information of its customers, staff, consultants, elected representatives and the security of its data.

Scope

6. This Policy applies to all persons employed at Central Coast Council, including Councillors, contractors, students, volunteers and agency personnel.

7. This Policy also applies to external organisations and their personnel who have been granted access to Central Coast Council Information & Technology (I&T) infrastructure, services and data.

8. The scope of the Policy includes Central Coast Council data held in any format or medium (paper based or electronic). The Policy does not apply to information that has been classified as Public.

9. 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.

Background

10. The Notifiable Data Breaches (NDB) Scheme, under the Federal Privacy Act 1988 (Privacy Act) establishes a mandatory data breach notification scheme that requires organisations covered by the Privacy Act to notify individuals and the Australian Information Commissioner about eligible data breaches.

11. Although the NDB Scheme applies primarily to Federal Government Agencies and private sector organisations regulated by the Australian Privacy Principles (APPs) under the Privacy Act, there are provisions that apply to NSW Public Sector Agencies. For Council, it is mandatory to apply the NDB Scheme to tax file numbers (TFN) it holds.

12. Notwithstanding the limited application of the NDB scheme, Council recognises the value of applying similar controls to other data that it holds and the importance of maintaining Council's reputation for privacy protection and the security of the data Council holds.

13. It is important to note that the IPC is only concerned with breaches that involve personal information. Data breaches that involve 'protected or confidential information' that is not 'personal information' do not need to be reported to the IPC.

General

14. A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to Council data, such as:

    a) accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick);

    b) unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or making unauthorised changes to data or information systems);

    c) unauthorised disclosure of classified material information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent;

    d) compromised user account (e.g. accidental disclosure of user login details through phishing);

    e) failed or successful attempts to gain unauthorised access to Council information or information systems;

    f) equipment failure;

g) malware infection; and/or

h) disruption to or denial of IT services.

15. A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

16. Containment of a data breach is a priority for the Council. All necessary steps possible will be taken to contain any data breach and minimise resulting damage.

17. If a third party is in possession of Council's data and declines to return it, Council may seek legal or other advice on possible action available to recover the data.

18. When recovering data, Council seek to ensure that copies have not been made by a third party or, if they have, that all copies are recovered.

19. The Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and reflect positively on the Council's reputation.

20. Notification demonstrates a commitment to open and transparent governance, consistent with the Council's approach.

21. In general, if a data breach creates a risk of harm to an individual/organisation, the affected individual/organisation will be notified. Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

22. The logistics 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.

23. The requirement for reporting a Data Breach are set out in the Data Breach Procedures.

Assessment and Responsibility

24. Where the relevant Director considers that the data breach is not a serious data breach, the responsible Unit Manager will conduct the Data Breach Response Plan in consultation with the Unit Manager Information and Technology.

25. Where the relevant Director considers that the data breach may be a serious data breach, the Response Team will convene in accordance with Council's *Data Breach Procedures*.

26. The Response Team will be responsible for conducting the Data Breach Response Plan as set out in Council's *Data Breach Procedures*.

27. The relevant Director and/or Unit Manager Information and Technology will lead the Response Team and may seek advice from other members of staff as appropriate.

28. It is not necessary that all members of the Response Team be included in all data breach responses, however, where a Directorate is affected or involved in a breach, or where a Directorate can assist in mitigating the harm caused by a breach, a listed or delegated primary or secondary contact must be involved in the response.

29. The Response Team must act promptly to appoint someone to lead the initial investigation. This person must be suitably qualified and have sufficient authority to conduct the initial investigation. In some instances, this may be a member of the Response Team or, as determined by the members of the Response Team, it will be a person most suitably qualified to carry out the initial investigation.

30. If, after evaluating the data breach, the Response Team considers that the breach is not a serious data breach, the responsible Unit Manager will be responsible for conducting the Data Breach Response Plan in consultation with the Unit Manager Information and Technology.

31. The Chief Executive Officer must be advised of any potential serious data breach by the relevant Director or the Unit Manager Information and Technology or their delegate.

Data Security

32. Council is committed to ensuring, as far as practicable, that the data it holds is secure from potential data breaches.

33. Council will regularly review, develop, maintain and test its systems and procedures to support data security and this Policy.

Review

Compliance, monitoring and review

34. 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.

35. This Policy will be reviewed every three years.

Records management

36. Staff must maintain all records relevant to administering this policy in a recognised Council recordkeeping system.

Definitions

Terms not defined in this document may be in a Council glossary or else state the terms and definitions as below.

37. In this policy:

Data breach means any failure that causes or permits, or has the potential to cause or permit, unauthorised access, disclosure, modification, use or misuse of data held by Council. Examples of data breach include, but are not limited to, the following:

a. A device containing data is lost or stolen.
b. Paper files or records containing data are lost or stolen.
c. A database is hacked.
d. Data is provided to the wrong person.
e. Data or information systems are used, accessed or modified without permission.
f. Users with permission look up data or information for unauthorised purposes eg: personal reasons.
g. Data is posted on a website without permission.
h. A user account is compromised.
i. Failed or successful attempts are made to gain unauthorised access to data or information systems.
j. Information systems or their protections fail or become unavailable.
k. Malware infects data or information systems.
l. Data is not disposed of securely and becomes public.
m. An individual deceiving Council into improperly releasing the personal information of another person.
n. Environmental breaches such as fire, storms and floods, biological agents and chemical spills and power outages.

Response Team means the relevant Director and/or the Unit Manager Information and Technology and any other appropriate Council Staff as determined by the Unit Manager Information and Technology.

Responsible Manager means the Manager responsible for the data subject to the breach.

Serious data breach means a data breach that is likely to result in serious harm to any individual or organisation, which may include, but is not necessarily limited to, serious financial, physical, psychological, emotional or reputational harm. Examples of serious harm include:

a. Financial fraud including unauthorised credit card transactions or credit fraud;

b. Identity theft causing financial loss or emotional and psychological harm;
c. Family violence;
d. Physical harm or intimidation;
e. Significant commercial or reputational damage due to release of commercially sensitive information.

Staff means Council's permanent, temporary or casual employees, volunteers, and contractors.

Related resources

38. Legislation:
    (a) *Privacy and Personal Information Protection Act 1998*
    (b) *Health Records and Information Privacy Act 2002*
    (c) *Data Sharing (Government Sector) Act 2015*
    (d) *Privacy Act 1988 (Cth)*
    (e) *State Records Act 1998 (NSW)*

39. Associated Documents:
    (a) Council's *Code of Conduct*
    (b) *Office of the Australian Information Commissioner – Data breach preparation and response guide – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*
    (c) *Information and Privacy Commission – Fact Sheet – NSW Public Sector Agencies and Notifiable Data Breaches*
    (d) *Information and Privacy Commission – Data Breach Guidance*

History of revisions

Amendment history	Details
Original approval authority details	Chief Executive Officer
	To protect the privacy and personal information of Council's customers, staff, consultants, elected representatives and the security of its data.
Version 1	Chief Executive Officer
	David Farmer, Chief Executive Officer Review to amend Position Titles as a result of the organisation restructure and to amend policy review period to three years.