POLICY

Name of Policy:	**Data Breach Policy**		
Adoption by Council:	**13 December 2023**	**Minute Number:**	**529/2023**
Last review date:	**November 2023**		
Review timeframe:	**2 years**		
Next scheduled review date:	**November 2025**		
Related legislation:	***Privacy and Personal Information Protection Act 1998 (PPIP Act)*** ***Health Records and Information Privacy Act 2002 (HRIP Act)*** ***Privacy Act 1988***		
Associated policies/documents:	**MidCoast Council Privacy Management Plan** **Cyber Security Framework** **Disaster Recovery Plan** **Business Continuity Management Policy and Plan** **Fraud and Corruption Control Framework** **Code of Conduct** **Risk Management Policy and Framework**		
Responsible division:	**Corporate Services**		

Policy objective

To provide guidance for responding to breaches of information held by Council and procedures for notifying any affected persons. In addition, this Policy aims to avoid or minimise any damage to individuals/organisations/Council and may prevent future breaches.

Policy statement

Council will manage the requirements of the mandatory notifiable data breaches scheme that applies under the *Privacy and Personal Information Protection Act 1998 (PPIP Act).*

Policy Coverage

This Policy applies to all Council staff; Councillors; volunteers; contractors and consultants.

Strategic Plan link

Community Outcome 4:
Strong leadership and good governance

4.1 The community has confidence in Council decisions and planning for the future	*4.1.2 Provide clear, accessible, timely and relevant information to the community about council projects and services.*

Legislation

Council has obligations under the *Privacy and Personal Information Protection Act 1998* (PPIP Act), the *Health Records and Information Privacy Act 2002* (HRIP Act) and the *Privacy Act 1988* including mandatory reporting obligations in respect of Data Breaches.

This Policy only relates to Data Breaches.

Council's *Privacy Management Plan* provides more information on how Council may collect, use and disclose Personal Information.

Policy content

What is a data breach?

A Data Breach occurs when there is an incident that has caused or has the potential to cause unauthorised access to or disclosure or loss of Council Held Information.
Examples include:

- accidental loss or theft of Council Held Information or equipment on which such Council Information is stored
- unauthorised use, access to or modification of Council Held Information or information systems
- unauthorised disclosure of classified Council Held Information, or Council Information posted onto the website without consent
- a compromised Council Officer's user account
- failed or successful attempts to gain unauthorised access to the Council's Information or information systems
- equipment failure
- malware infection
- malicious disruption to or denial of IT services

A Data Breach may occur directly by the Council or by a contractor or business partner of the Council who has custody of, or access to, Council Held Information.

This Policy applies to all Data Breaches and requires mandatory reporting of Eligible Data Breaches under the PPIP Act and Data Breaches in respect of tax files numbers (TFN), which must be reported under the Privacy Act.

The mandatory reporting obligations generally apply where there is unauthorised disclosure or access to Personal Information and it is reasonably considered that there could be serious harm to individuals to whom the information relates. Determining whether a Data Breach is subject to mandatory reporting obligations requires a specific assessment by Council's Privacy Officer and may also be determined based on legal advice.

Preparation for data breaches

Council maintains an effective and integrated risk management framework, allocating resources, responsibility and accountability to manage risks across the organisation in accordance with AS ISO 31000:2018. Refer to Council's Risk Management Policy and Framework for further information.

Council also has a range of supporting policies and stakeholder groups to control and mitigate exposures to breaches of data. This includes a Privacy Management Plan, Cyber Security Framework and Group, Data Security & Privacy Group, Disaster Recovery Plan, Business Continuity Management Policy and Plan, Fraud and Corruption Control Framework and Code of Conduct.

In addition to the policy controls, Council has a comprehensive set of information technology controls. This includes robust access controls, data encryption, network and endpoint security measures, data loss prevention systems, and incident response plans. An up-to-date inventory of assets is maintained, along with 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.

Training and awareness

To mitigate the risk of data breaches Council has established a comprehensive training program to educate employees about the risks associated with data breaches and their responsibilities in recognising, responding, reporting and preventing such incidents. Council conducts regular phishing simulation exercises to assess employee readiness for data breach incidents and raise awareness of the dangers of phishing and social engineering.

Contractors and third parties

Council will consider all contracts with contractors who may have access to, be provided with, or hold Council Held Information, to contain obligations requiring the contractor to:

- report Data Breaches to Council,
- take mitigating actions, and
- assist Council in undertaking assessments of the Data Breach.

Contracts may also identify who will notify any affected individuals and provide support in the event of a Data Breach.

For Data Breaches that involve other public agencies, the General Manager (or delegate) will directly liaise with other affected agencies in respect of any notification requirements for Mandatory Reporting Data Breaches.

Responding to a data breach

There are five steps in the process of responding to a Data Breach, which include:

1. Report and Triage
2. Contain
3. Assess and React

4. Notify relevant authorities and affected individuals
5. Review

Steps 1 - 3 will be followed for all Data Breaches. Steps 4 and 5 only need to be followed if the preceding steps result in any notification or review requirements. Each step will be considered, and to the extent appropriate, implemented in responding to a Data Breach.

Every response will need to be considered, holistically, and on a case-by-case basis, depending on the nature, severity and impact of the Data Breach.

Responding to Data Breaches	
1	**STEP ONE: Report and Triage** • Any Council Officer who becomes aware of a Data Breach will **immediately** notify the Relevant Manager or Director. • Where a Council Officer and/or a Relevant Manager or Director, believes or has reasonable grounds to believe that the Data Breach is a Mandatory Reporting Data Breach, the Relevant Manager or Director will notify the General Manager (or delegate) **immediately**. • When reporting a possible Mandatory Reporting Data Breach to the General Manager (or delegate), a Council Officer and/or a Relevant Manager or Director will also indicate whether in their opinion it is likely to take more than 30 days to determine if the Data Breach is a Mandatory Reporting Data Breach (if known). • For Non-Eligible Data Breaches, a Relevant Manager or Director will notify the Privacy Officer **within 24 hours**. • The Privacy Officer, on being notified of a Data Breach will contact Council's insurer.
2	**STEP TWO: Contain** • All Council Officers will take all immediate steps to contain any Data Breach, by limiting the extent and duration of the unauthorised access to or disclosure of Council Held Information, and preventing the Data Breach from intensifying. • This obligation is ongoing as other steps proceed.
3	**STEP THREE: Assess and React** **Assessment of whether the Data Breach is a Mandatory Reporting Data Breach** • If it is suspected that an Eligible Data Breach has occurred, the General Manager (or delegate) will assess whether an Eligible Data Breach has actually occurred (**Eligible Data Breach Assessment**). • The General Manager (or delegate) may appoint the Data Security & Privacy Group to assist in this regard. • After completing an Eligible Data Breach Assessment, the General Manager (or delegate) will make a final decision on whether the Data Breach is, or there are reasonable grounds to believe the Data Breach is an Eligible Data Breach. • The General Manager (or delegate) will also assess and consider whether a Data Breach is a Commonwealth Notifiable Data Breach. Commonwealth Notifiable Data Breaches are specific to unauthorised access or disclosure of TFNs. Council has 30 days to complete this assessment from the date of the

initial report of the Data Breach.

General Assessment

- Council will conduct a preliminary assessment of a Data Breach by gathering all relevant information in respect of the Data Breach.
- Council will then evaluate the risks of the Data Breach for all Data Breaches.
- Factors to consider include:
  - What Council Held Information has been lost or disclosed?
  - What is the nature of the Council Held Information that has been lost or disclosed?
  - What was the cause of the Data Breach?
  - Who is affected by the Data Breach?
  - What combination of information was lost? Certain combinations of types of Personal Information can lead to increased risk.
  - How long the Information has been accessible? The length of time of unauthorised access to, or unauthorised disclosure will increase risks of harms to individuals.
  - How many individuals were involved? The scale of the Data Breach will likely affect the Council's assessment of likely risks.
  - If the Data Breach involves TFN information?
  - Was it a one-off incident or does it expose a more systemic vulnerability?
  - What steps have been taken to contain the Data Breach? Has the Council Held Information been recovered? Is the Council Held Information encrypted or otherwise not readily accessible?
  - What is the foreseeable harm to affected individuals/organisations?
  - Who is in receipt of the Council Held Information? What is the risk of further access, use or disclosure, including via media or online?
  - Are other public agencies involved in the Data Breach?

Where a third party has gained possession of Council Held Information and declines to return it, the General Manager (or delegate) will engage external legal advice on what action can be taken to recover the Council Held Information. When recovering Council Held Information, the Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

Council will ensure that all actions to manage, contain, mitigate and remediate the impact of a Data Breach to prevent future Data Breaches are considered and implemented.

4

STEP FOUR: Notify

Eligible Data Breach Notification

The General Manager (or delegate) will notify the Privacy Commissioner **immediately** after determining that a Data Breach is an Eligible Data Breach.

- Notification to the Privacy Commissioner will be made in the approved form by the Privacy Commissioner as published on the IPC's website.
- The General Manager (or delegate) and Data Security & Privacy Group (if appointed) will notify Affected Individuals **as soon as practicable** after identifying an Eligible Data Breach.
- The General Manager (or delegate) and Data Security & Privacy Group (if appointed) will determine how to notify, and oversee the notification to Affected Individuals of the Eligible Data Breach in accordance with this Policy.

Commonwealth Notifiable Data Breach Notification

- The General Manager (or delegate) and Data Security & Privacy Group (if appointed) will notify the Office of the Australian Information Commissioner (OAIC) and any affected individuals **as soon as practicable** after identifying a Commonwealth Notifiable Data Breach.
- The General Manager (or delegate) and Data Security & Privacy Group (if appointed) will determine how to notify and oversee the notification made to the OAIC and any affected individuals of the Commonwealth Notifiable Data Breach.

Voluntary Data Breach Notification for Non-Eligible Data Breaches

- As a matter of best practice, Council will also consider voluntary Data Breach notification to the IPC, affected individuals and others (if the Data Breach is a Non-Eligible Data Breach).

Notification of individuals affected by a Mandatory Reporting Data Breach

- Council will notify affected individuals directly, by telephone, letter, email or in person. Indirect notification - such as information posted on the Council's website, a public notice in a newspaper, or a media release will generally occur where the contact information of individuals who are affected are unknown, or where direct notification is prohibitively expensive or could cause further harm.
- Council will maintain a public notification register in accordance with 59N(2) and s59P of the PPIP Act. Council will also maintain an internal register for Eligible Data Breaches.

All Notifications

- Council will at all times and for every Data Breach, consider other internal and external notifications and approvals, and communicate with such external agencies and stakeholders as is reasonably required in the individual circumstances of a particular Data Breach (e.g. the Police, Department of Customer Service, Cyber Security NSW, the Australian Tax Offices etc.).
-

5

STEP FIVE: Review

- Council will conduct a detailed review of all Data Breaches to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.
- From its review of a particular Data Breach, Council will undertake any recommended steps to further mitigate and remediate Council's procedures, policies and IT systems to prevent future Data Breaches.
- A post incident review will consider:
  - a cause analysis of the Data Breach;
  - security audit of both physical, technical and cyber security controls;
  - review of Council's risk management policies and procedures;
  - review of employee training practices;
  - review of contractual obligations with contracted service providers;
  - any other review considerations, recommendations or guidelines published by the IPC or Privacy Commissioner.
- A report of all Data Breaches considered to be serious and all Mandatory Reporting Data Breaches will be made to Council's Audit Risk and Improvement Committee and to Council.
- This Policy will be reviewed, tested and updated in accordance with Council's

	established policy review processes or as required by best practice or legislation changes.

Communications

All internal communications relating to a Data Breach are to be via Council's Privacy Officer (Manager Governance) or through Council's Communications Team. All external communications relating to a Data Breach are to be via Council's Communications Team only.

Definitions

Affected individual means an "affected individual" as defined in the PPIP Act.

Commonwealth Notifiable Data Breach means an "eligible data breach" as defined in the Privacy Act.

Council Held Information means any Personal Information in whatever form (including hard copy, and electronically held information), which is held by Council or is otherwise in the possession or control of Council.

Council Officer means any officer or employee of Council.

Data breach means the unauthorised access to, or inadvertent disclosure, access, modification, misuse or loss of, or interference with Personal Information, and in this Policy includes a potential Data Breach.

Data Security & Privacy Group is a group of identified stakeholders (endorsed by Senior Executive) to consider matters relating to Data Security and Privacy Information.

Eligible Data Breach means an "eligible data breach" as defined in s59D of the PPIP Act.

HRIP Act means the *Health Records Information and Privacy Act 2002* (NSW).

IPC means the Information and Privacy Commission of NSW.

IT means information technology

OAIC means the Office of the Australian Information Commissioner.

Mandatory Reporting Data Breach means an Eligible Data Breach or a Commonwealth Notifiable Data Breach.

Non-Eligible Data Breach means any Data Breach that is not a Mandatory Reporting Data Breach.

Notifiable data breach means a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner.

Personal information means information or an opinion about an individual who is identified, or who can reasonably be identified, from the information, whether or not the information or opinion is true or recorded in a material form, and includes sensitive information.

PPIP Act means the *Privacy and Personal Information Protection Act 1988* (NSW).

Privacy Act means the *Privacy Act 1988* (Cth).

Privacy Commissioner means the NSW Privacy Commissioner, or as otherwise defined in the PPIP Act.

Privacy Officer is delegated by the General Manager and is the Manager Governance.

Relevant Manager or Director means the manager or director to whom a Council Officer reports, or the manager or director with responsibility for a contract with a third-party contractor.

Response Team means the team established for the purposes of responding to a Data Breach that includes the General Manager, Director Corporate Services, Manager Governance, Manager Information Technology, and Manager Engagement, Communication & Education.

Sensitive information means information or an opinion that is also personal information, about a person's racial or ethnic origin, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practises, criminal history, health information, and genetic and biometric information.

TFN means a tax file number as defined in Part VA of the *Income Tax Assessment Act 1936* (Cth).

References and related documents

- MidCoast Council Privacy Management Plan
- Cyber Security Framework
- Disaster Recovery Plan
- Business Continuity Management Policy and Plan
- Fraud and Corruption Control Framework
- Code of Conduct

Responsible officer (position)

Manager Governance as Council's Privacy Officer