14.4 Endorse for public exhibition: Draft Mandatory Notification of Data Breach Policy

CSP Objective: Outcome 5.2: Governance is transparent and builds trust

CSP Strategy: 5.2.2 Communicate openly and honestly with the community to build a relationship based on transparency, understanding, trust and respect.

Delivery Program: 5.2.2.1 Council's external and internal communications, including web and intranet assets, deliver efficient online services for users, facilitate effective engagement between our community and Council, meet legal requirements, and industry and accessibility standards.

Summary

The proposed Mandatory Notification of Data Breach Policy has been drafted to provide the framework to assist Council employees and our community to understand Council's response to data breach incidents.

The Policy adheres to the requirements of the mandatory notification provisions under Part 6A of the Privacy and Personal Information Protection Act, which comes into effect on 28 November 2023.

Financial implication

The Mandatory Notification of Data Breach Policy is an administrative policy and does not impact the budget. The policy however prescribes for timely and comprehensive response to data breaches to limit possible impact to security of council records and systems including financial data.

Risk implication

The Mandatory Notification of Data Breach Policy is aligned with reputational, financial, operational and reputational risk mitigation strategies.

- It demonstrates to our customers that we have processes in place to identify and manage data breaches, and that these are deployed without delay to minimise any potential damage
- The process of assessment, notification and remediation will strengthen data breach and privacy processes, preventing future breaches and minimising further risk for council.
- It reinforces the importance on accountability for the protection of personal information internally to our employees, to promote a privacy positive culture
- It demonstrates to the public that council views the protection of information as a priority, helping to maintain public trust.

Policy

Draft Mandatory Notification of Data Breach Policy

Consultation (internal)

Management Leadership team

Executive Leadership Team

Communication/Community engagement

It is proposed that the Draft Mandatory Notification of Data Breach Policy be placed on public exhibition for a period of 28 days to allow the community to provide feedback.

Attachments

1 DRAFT Mandatory Notification of Data Breach Policy⇩

Enclosures
Nil

RECOMMENDATION

That Council:

1. proceed to public exhibition of the Draft Mandatory Notification of Data Breach Policy for a period of 28 days.
2. note if submissions are received during the exhibition period a further report will be provided on any proposed amendments to the Draft Mandatory Notification of Data Breach Policy.
3. adopt the Mandatory Notification of Data Breach Policy if no submissions are received on the day after the completion of the public exhibition period.

Background

Council's Privacy Management Plan details when and how council manages personal information of our employees and customers. It makes reference of the requirements to keep a register of privacy breaches but does not detail the current procedures of privacy breach management.

This policy strengthens our current procedures and aligns to reforms under the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA)

The Draft Mandatory Notification of Data Breach Policy is attached for Councillors' consideration.

KIAMA MUNICIPAL COUNCIL
your council, your community

DRAFT Mandatory Notification of Data Breach Policy

Policy Owner/Responsible Officer	Public Officer
Department	People & Performance
Date adopted/endorsed	21 November 2023
Resolution number (if applicable)	XX
Next review date	D Month Year
TRIM reference	XX

Contents

Policy Statement/Objectives

Kiama Municipal Council is committed to providing staff with guidance on data breaches in accordance with the requirements of the PPIP Act.

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches. Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

The objective of the policy is to outline Kiama Council's approach to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing, and managing eligible data breaches.

RESPECT · INTEGRITY · INNOVATION · TEAMWORK · EXCELLENCE ·

The purpose of this policy is to provide guidance to Council staff on data breaches of Council held data in accordance with the requirements of the PPIP Act and to set out how Council will respond to data breaches involving personal information. Council acknowledges that not all data breaches will be eligible data breaches but regardless, council takes all data breaches seriously. The policy details:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

Effective breach management, including notifications assists Council in avoiding or reducing possible harm to both the affected individuals/organisations and Council, and may prevent future breaches.

Scope

This policy applies to all staff and contractors of Kiama Municipal Council. This includes temporary and casual staff, private contractors and consultants engaged by Council to perform the role of a public official. This policy also applies to third party providers, who hold personal and health information on behalf of Council.

This policy will be reviewed in 12 months' time or where improvements are identified in response to a data breach whichever occurs sooner.

References

- Privacy and Personal Information Protection Act 1998 (PPIP Act) (NSW) ss. Part 6A, 59D, 59N(2), 59ZD
- NSW Privacy and Personal Information Protection Regulation 2019
- NSW Government Information Classification, Labelling and Handling Guidelines (July 2015)
- Privacy and Personal Information Protection Act 1998
- Privacy and Personal Information Protection Amendment Bill 2021
- Health Records and Information Privacy Act 2002
- State Records Act 1998 (NSW)
- Government Information Classification and Labelling Guidelines 2013 (NSW)

Consultations

- Information and Privacy Commission NSW Electoral Commission

Definitions

Term	Definition
Personal information	The definition of personal information for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act). This means that for the purposes of the MNDB Scheme, 'personal information' means *information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion* and includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service
Data breach	A data breach occurs when personal information held by an agency (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. This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach. A data breach may occur as the result of malicious action, systems 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)
Human error	Examples of data breached include: • when a letter or email is sent to the wrong recipient • when system access is incorrectly granted to someone without appropriate authorisation • when a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced • when staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
System Failure	Examples of data breaches include: • where 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 • where systems are not maintained through the application of known and supported patches

Malicious or criminal attack	Examples of data breaches include: • cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information • social engineering or impersonation leading into inappropriate disclosure of personal information • insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions • theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

Variation and review

Council reserves the right to review, vary or revoke this policy.

Review History

Date reviewed	Date adopted/ endorsed	Brief detail of amendments
		This is a new policy.

POLICY

1. Eligible Data Breach

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:**

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**

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.

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

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- the level of sensitivity of the personal information accessed, disclosed or lost

- 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
- 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)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

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.

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 the agency's position would identify as a possible outcome of the data breach.

2. Roles and Responsibilities

The following employees have identified roles under the Mandatory Notification of Data Breach Policy:

- the Governance Coordinator is responsible for implementing this Policy, reporting data breaches to the Chief Executive Officer and all notifications and actions for eligible data breaches
- the Governance Coordinator is responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches
- the Manager Communications and Engagement and Manager People and Performance will provide advice on the communication strategy and messaging to affected individuals and external reporting agencies
- all Kiama Council Employees have a responsibility for immediately reporting a suspected data breach in accordance with this policy.

3. Systems and Processes for managing a data breach

Kiama council has established a range of systems and processes for preventing and managing data breaches.

Council's IT network and infrastructure is managed by (ICT) Information, Customers and Technology who have implemented several cyber security measures to mitigate the risk of data breaches. This has included projects to increase cyber security maturity, cyber security training for all staff (including threat trends), Data Loss Prevention, and procedures for the sharing of personal and sensitive information.

Council will store personal information for as long as required by the General Retention Disposal Schedule for Local Government in accordance with the State Records Act 1989 and Council's Records Management System. It will then be disposed of securely. Council will store personal information securely and protect it from unauthorised access, use or disclosure by applying security access levels to Council's electronic records management system.

Kiama 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 data breaches to Council and Information and Privacy Commission.

This plan establishes a process for reporting, managing and responding to data breaches including notifications to the Privacy Commissioner and affected individuals. The plan also includes steps for reviewing, responding, and developing remedies for preventing data breaches.

Kiama Council also maintains an internal register of 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.

Presentations and training will be provided to Council staff on the MNDB Scheme and reporting and managing data breaches. Kiama Council will continue to review the training needs of staff with respect to data breaches and provide training in reporting, managing and responding to data breaches.

Council has included the risk of a cyber security incident (which may involve a data breach) within its Risk Register and established controls to mitigate this risk and its impact. The loss of IT systems because of a cyber security incident is included in Council Strategic Improvement Plan 2. Council also conducts cyber security exercises to test the responsiveness of the plan.

4. Reporting and responding to a data breach

The Governance Coordinator must be informed of any data breach to ensure the application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

There are five key steps required in responding to a data breach. Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Governance Coordinator will liaise with Council and/or its service providers to address and respond to identified data breaches.

4.1 Step one: Initial report and triage

An employee, contractor or third-party provider is to notify the Governance Coordinator within one business day of becoming aware that a data breach has occurred and provide information about the type of data breach. The Governance Coordinator will notify the CEO immediately of a suspected eligible data breach. The Manager People and Performance will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme, complete the Data Breach Report and Action Plan and include all data breaches in the Internal Data Breach Register (TRIM 21/46469). Members of the public are also encouraged to report any data breaches to Kiama Council in writing by using the contact options available on our website.

The data breach response team will be activated in the event of a complex or unidentified cause of the breach and significant reputational risk for Council. The team will be made up of (ICT) Information, Customers and Technology, Governance, Risk, Human Resources and will report to the CEO.

4.2 Step two: Contain the breach

Containing the breach is prioritised by Council. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords.

If a third-party is in possession of the data and declines to return it, it may be necessary for Council to seek legal, forensic or other advice on what action can be taken to recover the data. When recovering data, Council will make sure that copies 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.

4.3 Step three: Assess and mitigate

To determine what other steps are needed, 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. The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. The Governance Coordinator and Manager People and Performance will prepare a report and provide to the CEO. Data Breach Report and Action Plans are to be saved in Council electronic record keeping system.

The Governance Coordinator will be responsible for the implementation of proposed actions and recommendations.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list. Given Councils regulatory responsibilities, release of case-related personal information will be treated very seriously.

A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- Who is affected by the breach? The Council assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- What was the cause of the breach? The Council assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Questions include: Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?

- What is the foreseeable harm to the affected individuals/organisations? The Councils assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information personal information subject to special restrictions under s.19(1) of the PPIP Act), if could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage Council's reputation?

- Guidance issued by the Privacy Commissioner on assessing eligible data breaches Upon becoming aware of a possible data breach, Council will consider any guidance issued by the NSW Privacy Commissioner.

- To mitigate the breach, Kiama Council will consider the following measures:
- Implementation of additional security measures within Council's own systems and processes to limit the potential for misuse of compromised information.
- 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.
- 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.

4.4 Step four: Notify

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered. There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.

2. Determine whether an exemption 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. Council and the IPC has produced guidance to agencies on exemptions from notification.

3. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.

4. Provide further information to the Privacy Commissioner.

Kiama Council recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations and is consistent with the Council regulatory role. Notification demonstrates a commitment to open and transparent governance, consistent with Council's approach. 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 upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable.

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. Considerations include the following:

When to notify

Individuals/organisations affected by a data breach will be notified as soon as practicable. Whilst this policy sets a target of notification within 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

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on Kiama Council's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). A record of any public notification of a data breach will be published on Councils website and recorded on the Public Data Breach Register for a period of twelve months.

What to say

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred
- the personal information included in the breach
- the amount of time the personal information was disclosed for
- actions that have been taken or are planned to secure the information, or to control and mitigate the harm
- recommendations about the steps an individual should take in response to the breach
- information about complaints and reviews of agency conduct
- the name of the agencies that were subject to the breach
- 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:

Kiama 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.

Depending on the circumstances of the data breach this could include:

- NSW Police Force and/or Australian Federal Police, where the IPC suspects a data breach is a result of criminal activity
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident

- The Office of the Australian Information Commissioner, where a data breach may involve agencies under the Federal jurisdiction
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a data breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers, where a data breach may have an impact on these organisations, their functions and their clients
- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

4.5 Step five: Further Review

Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Depending on the nature of the breach step five may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three above.

Preventative actions could include a:

- review of Council's IT systems and remedial actions to prevent future data breaches
- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be reported to the CEO and documented in Council's electronic record keeping system. Consideration will be given to reporting relevant matters to Council's Audit, Risk and Improvement Committee.

Related Forms/Documents

- Privacy Management Plan
- Councils Operational Plan
- Council Business Continuity Plan
- Strategic Improvement Plan 2
- KMC Style Guide.

Attachments

Nil	

Authorisation

Name: Title of person authorising OR ELT OR Council Resolution No: ****

Date: Date endorsed by ELT or adopted by Council