Data Breach Determination

Purpose / Statement

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme.

Under the scheme, Council is required to prepare and publish a Data Breach Determination (DBD) for managing eligible data breaches.

The purpose of this determination is to provide guidance to Council staff in responding to an eligible data breach of Council held personal information.

This sets out Council procedures for managing an eligible data breach, including:

- providing examples of situations considered to constitute an eligible data breach
- the steps involved in responding to an eligible data breach
- the considerations around notifying persons whose privacy may be affected by the breach.

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

Principles

What is an eligible data breach?

An 'eligible data breach' occurs where:

- 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
- 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 MNDB scheme applies to breaches of 'personal information' as defined in section 4 of PPIPA, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It also applies to 'health information,' defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIPA), about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Examples of activities that may lead to an eligible data breach are:

- accidental loss or theft of classified material data or equipment on which personal information is stored (e.g. loss of paper record, laptop, tablet or mobile phone, compact disk or USB stick)
- 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 make unauthorised changes to data or information systems)

- unauthorised disclosure of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted on to Council's website without consent
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to Council information or information systems
- equipment failure
- malware infection
- disruption to or denial of IT services.

Any breach of personal information should be reported immediately to the Manager, Information Access & Privacy or the Office of General Counsel.

Preparation for a data breach

A Data Breach Response Plan (DBRP) has been prepared to guide Council through the process for dealing with a data breach. It covers key controls to ensure the data breach is effectively managed. A copy of the DBRP is provided as an appendix to this determination.

The DBRP enables Council to contain, assess and respond to data breaches in a timely fashion and help mitigate potential harm.

Training and awareness

Most data breaches are at least partially the result of human factors, such as human error or cyber attacks that result from human compromise. To mitigate this risk, Council provides mandatory privacy and cyber security awareness training.

Reporting breaches

If an eligible breach occurs, Council must report it to the Privacy Commissioner and include the following:

- A description of the type(s) of personal information
- Whether other agencies were involved in the breach
- Whether the breach is a cyber incident
- An estimate of the cost of the breach to Council
- The number of individuals:
    - Involved in the breach
    - Notified of the breach
- Whether those notified have been advised about complaints and review processes.

If notification occurs before the completion of the incident response or for some other reason, the report can be limited to the information available at the time. In such cases, the Privacy Commissioner must be provided further information in a follow up notification.

There are exemptions that apply to this process. They are:

- Where an eligible data breach affects multiple public sector agencies, and another agency has undertaken to notify individuals. Both agencies must still conduct their own assessment, containment and mitigation, and notify the Privacy Commissioner.
- Where notification of the eligible data breach would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or a tribunal.
- Where the agency has taken mitigation action that successfully prevents serious harm from occurring, so that a reasonable person would conclude that the breach is no longer likely to result in serious harm to an individual.
- Where notification would be inconsistent with a secrecy provision in another Act.
- Where notification would create a serious risk of harm to an individual's health or safety.
- Where notification would worsen the agency's cyber security or lead to further breaches.

Council must advise the Privacy Commissioner if relying on one of these exemptions and record the decision process.

Third party data sharing that includes personal information

Council is at times required to share personal information with third parties, for example, to allow the third party to provide Council with a service that assists Council in optimising the services it provides to the community.

Prior to sharing any personal information with a third party to outsource a Council function, the following tasks may be undertaken:

- Data sharing agreement
- Privacy impact assessment

For further details and advice on third party data sharing arrangements, please contact the Manager, Information Access and Privacy.

How data breaches will be managed

If a staff member reports a data breach, the DBRP is activated. There is no uniform method for responding to a data breach, although the actions taken following a data breach should follow four key steps.

Step 1 - Contain the breach and conduct a preliminary assessment

The aim of this step is to limit the impact of the breach. Consideration of the following may assist in determining how the breach can be contained:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

Some basic information should be collected, such as:

- Time and date of the breach
- Context of the information
- Person's name reporting the breach

Step 2 - Evaluate the risks associated with the breach

The aim of this step is to understand the risks posed by a data breach and how to manage them. In this stage, the risk of harm to individuals can be determined. The following should be considered:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the likelihood of those persons who have access to personal information:
    - causing, or intending to cause harm, or
    - circumventing security measures protecting the information, and
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

Step 3 - Notification

Determine if notifying affected individuals should be conducted. To determine whether to notify, the following should be considered:

- Council is required to notify individuals and the Privacy Commissioner about data breaches that are likely to result in serious harm.
- Council may not have obligations under the MNDB scheme, but decide to notify affected individuals in certain circumstances
- The method of notification, including:
    - what information is provided in the notification
    - how the notification will be provided to individuals
    - who is responsible for notifying individuals and creating the notification
    - who else other than affected individuals (and the Commissioner if the notification obligations of the MNDB scheme apply) should be notified
    - where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public
    - whether the incident triggers reporting obligations to other entities.

The aim is to reduce any harm that may be suffered by affected individuals. Notification provides affected individuals with the chance to protect their personal information following a data breach. It also provides Council with an opportunity to work with affected individuals to assist them in limiting the damage the breach may cause them.

Step 4 - Prevent future breaches

Conduct full investigation including:

- address issues causing the breach
- review and update relevant documents (e.g. policies and procedures)
- conduct a security audit of both physical and technical security controls
- review contractual obligations with contracted service providers (if relevant having regard to the circumstances of the breach)
- update IPC of actions to date and keep IPC informed as new information about the breach becomes available
- any other actions deemed necessary by council.

Roles and responsibilities

An example of the Data Breach Response Team membership is as follows:

Team Member	Expertise	Role
Contract/Service Owner	Incident Controller	Lead incident response
Manager Information Access & Privacy	SME – Organisational Support	Provide organisational support and direction as and when required
Manager, Systems Development & Support	SME – IT Systems	Provide subject matter expertise
Chief Information Security Officer	SME – IT Infrastructure	Provide subject matter expertise
Manager, Communications	Communications Lead	Oversee internal and external communications
General Counsel	Legal Representative	Provide legal advice as required
Chief Information Officer	Executive Team Representative	Advise CEO and other Executives of situations as and when required

It is the responsibility of all staff to watch for and report data breaches immediately. If unsure, the staff member should report the potential data breach for assessment by the Manager, Information Access & Privacy or the Office of General Counsel.

Recordkeeping requirements

Documents created by the Response Team should be saved in the following TRIM container:

C000199: CORPORATE MANAGEMENT - Policy - Administrative and Operational Policies for Common Administrative Functions - Privacy Management Plan and Privacy Matters - Information Management - Information and Digital Technology

Incident register

Council is required to establish and maintain an internal register of eligible data breaches. This register should record every eligible breach including the following:

- who was notified of the breach
- when the breach was notified

- the type of breach
- details of steps taken by Council to mitigate harm done by the breach
- details of the actions taken to prevent future breaches
- the estimated cost of the breach.

Public notification register

Council is required to maintain a public notification register of any notifications and publish it on our website. Entries must be added to the register in two sets of circumstances:

- a public notification must be made by Council if it is unable, or it is not reasonably practicable, to notify any or all the individuals affected by the breach directly, or
- where the CEO decides to make a public notification. Council should note that the issuing of a public notification in these circumstances does not excuse it from the requirement to make direct notifications to affected individuals if it is reasonably practicable to do so.

The publication notification register contains the following:

- the date the breach occurred
- a description of the breach
- the type of breach (unauthorised access, unauthorised disclosure or loss of information)
- how the breach occurred
- the type of personal information that was impacted by the breach
- actions taken or planned to ensure that personal information is secure or to mitigate harm to individuals
- recommended steps individuals should take in response to the breach
- date the public notification was published
- where to contact for assistance or information
- a link to the full public notification.

Any public notification must be published on the public notification register and remain available for at least 12 months after the date of publication.

Scope and application

This Determination applies to all employees, agents and officers of Northern Beaches Council, as well as all Councillors when performing their role as a Councillor.

References and related documents

- Privacy Management Plan

- Guide - Mandatory Notification of Data Breach Scheme: Guide to managing data breaches in accordance with the PPIP Act
- Guide - Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy

Responsible Officer

Chief Information Officer

Review Date

28 November 2024

Revision History

Revision	Date	Change	TRIM #
1	27 March 2024	Change references from Operational Policy to Determination	2023/490903
2			
3			
4			

NORTHERN BEACHES COUNCIL

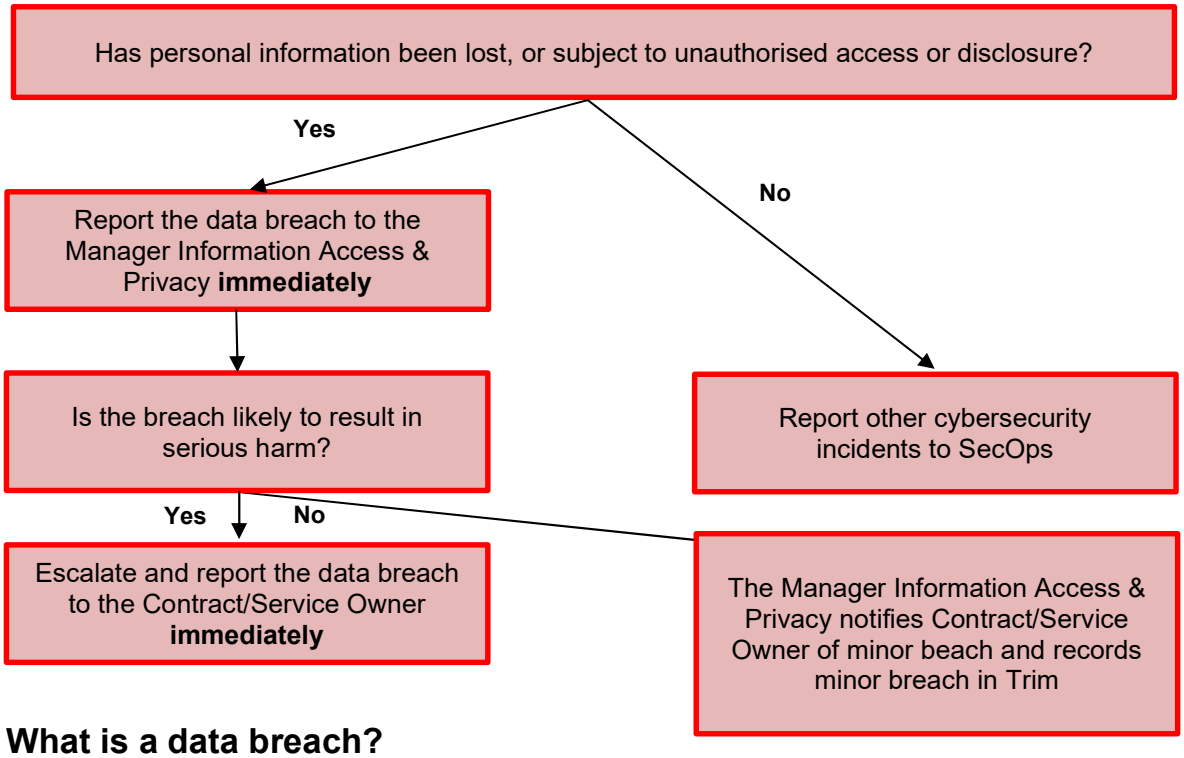
DATA BREACH RESPONSE PLAN

Data breach Response plan overview

This data breach response plan outlines definitions, sets out procedures and clear lines of authority for Council staff if Council experiences a data breach, or suspects that a data breach has occurred.

This response plan is intended to enable Council to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist Council to respond to a data breach.

Escalation Flowchart



What is a data breach?

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information is information or an opinion about an identified or reasonably identifiable individual. Data breaches may include (but are not limited to) unauthorised access by a third party, information accidentally being uploaded to a public website or a laptop or USB drive containing personal information being lost or stolen and can be

caused by or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies or organisations.

Which data breaches are notifiable?

Not all data breaches require notification. The Mandatory Notification of Data Breach Scheme (MNDB scheme) only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates. The purpose of this plan is to enable that assessment to be undertaken and for Northern Beaches Council (Council) to meet its reporting obligations. Where an eligible data breach is assessed as having occurred then the Data Breach Response Team will act as quickly as possible.

Northern Beaches Council Data Breach Response Team

Response Team membership (example)

Team Member	Expertise	Role
Contract/Service Owner	Incident Controller	Lead incident response
Manager Information Access & Privacy	SME – Organisational Support	Provide organisational support and direction as and when required
Manager, Systems Development & Support	SME – IT Systems	Provide subject matter expertise
Chief Technology & Operations Officer	SME – IT Infrastructure	Provide subject matter expertise
Manager, Communications	Communications Lead	Oversee internal and external communications
General Counsel	Legal Representative	Provide legal advice as required
Chief Information Officer	Executive Team Representative	Advise CEO and other Executives of situations as and when required

Response Team membership will vary, depending upon the business unit involved and type of data breach. The above example will apply when the data breach is IT system related. There may be cases where a data breach occurs (e.g. involving hard copy documents) and no IT systems are involved.

Assessing suspected data breaches

If any Northern Beaches Council staff member suspects or becomes aware of a data breach, this plan is activated and must be followed. The plan requires a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm. The following chart outlines the staff roles involved in assessing a data breach.

NORTHERN BEACHES COUNCIL EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED

The Data Breach was discovered by Council staff member, OR Northern Beaches Council is alerted of the breach.

↓

WHAT SHOULD THE NORTHERN BEACHES COUNCIL STAFF MEMBER DO?

- Immediately notify the Manager Information Access & Privacy of the suspected data breach.
- Record and advise the Manager Information Access & Privacy of the time and date the suspected data breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

↓

WHAT SHOULD THE MANAGER INFORMATION MANAGEMENT DO?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team.

↓

ALERT NORTHERN BEACHES COUNCIL DATA BREACH RESPONSE TEAM INCIDENT CONTROLLER

Controller convenes Response Team

When should the Manager Information Access & Privacy escalate a data breach to the Data Breach Response Team?

Manager Information Access & Privacy to use discretion in deciding whether to escalate to the Response Team.

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (**Response Team**).

In determining whether to escalate data breaches to the Response Team, the Manager Access & Privacy should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in Northern Beaches Council processes or procedures?
- Could there be media or stakeholder attention resulting from the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the Manager Access & Privacy to notify the Incident Controller who is to form a Response Team.

Manager Information Access & Privacy to inform the Incident Controller of minor breaches.

If the Manager Access & Privacy decides not to escalate a minor data breach or suspected data breach to Contract/ Service Owner to form the Response Team for further action, the Manager Access & Privacy should:

- **send a brief email to the Contract/Service Owner** – that contains the following information:
  - description of the breach or suspected breach
  - action taken by the Manager Access & Privacy to address the breach or suspected breach
  - the outcome of that action, and
  - the Manager Access & Privacy's view that no further action is required

- **save a copy of that email in the following folder:**
  C000199: CORPORATE MANAGEMENT - Policy - Administrative and Operational Policies for Common Administrative Functions - Privacy Management Plan and Privacy Matters - Information Management - Information and Digital Technology in CM10

DATA BREACH RESPONSE PROCESS

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected data breach.

- **STEP 1: Contain the breach and do a preliminary assessment –** Manager Access & Privacy to capture – time and date of breach, type of personal information involved, cause and extent of breach, context of affected information.
- **STEP 2: Evaluate the risks associated with the breach –** Manager Access & Privacy to notify Contract/Service Owner of breach, describe actions taken so far and the outcome of

that action, a view of the seriousness of the breach for Manager Access & Privacy to the Contract/Service Owner and if any further action is required
- **STEP 3: Notification** – decide if a notifiable breach, based on the likelihood of serious harm, notify IPC**.** Decide if contacting affected individuals should occur.
- **STEP 4: Prevent future breaches –** conduct full investigation, address issue that caused the breach, update data breach response plan (if required), look and possibly update relevant policies and procedures, review - staff training, expertise in response team, communications and media strategy and advise IPC of actions to date

The Response Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. Refer to the checklist at the end of this plan.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach. The checklist at the end of this plan is intended to alert the Response Team to a range of considerations when responding to a data breach and guide the Response Team in the event of a data breach.

Evaluating a serious risk of harm to an individual

In evaluating whether there is a serious risk of harm to an individual whose information is the subject of a data breach, the Response Team must consider:

- what type of personal information is involved (and in particular, whether it is sensitive information);
- whether there are any protections that would prevent the party who receives (or may have received) the personal information from using it (for example, if it is encrypted);
- the nature of the harm that could arise from the breach, for example whether an individual was reasonably likely to suffer:
    - identity theft;
    - financial loss;
    - a threat to their physical safety;
    - a threat to their emotional wellbeing;
    - loss of business or employment opportunities;
    - humiliation, damage to reputation or relationships; or
    - workplace or social bullying or marginalisation;
- what steps have been taken to remedy the breach (and how certain Northern Beaches Council is that they are effective). This must be done as soon as practicable to lessen the likelihood of harm.
- complete an assessment that determines if there are reasonable grounds to consider the breach may result in serious harm to anyone.
- ensure the breach has been fully contained
- engage appropriate expertise to assist with conduct of the assessment
- the risk profile of the information involved
- the risk to the individuals involved (eg risk of family violence)
- the amount of time that has passed between the breach and containing it
- consider if it was it an isolated or reoccurring incident
- likelihood the person in receipt of the information will cause harm
- any ongoing risks created by the breach
- the extent to which the risk has been mitigated by actions taken

Notifying the Office of the NSW Information and Privacy Commission

In the event that the Response Team decides there has been a data breach and there is a real risk of serious harm to affected individuals the Response Team must prepare a statement that includes:

- Northern Beaches Council's Manager Information Access & Privacy – chris.wilson@northernbeaches.nsw.gov.au or 02 8495 6179
- a description of the data breach;
- the kind of information concerned; and
- recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

The statement must be submitted to IPC via email to ipcinfo@ipc.nsw.gov.au as soon as reasonably practical.

Notifying the individuals affected

As soon as reasonably practical after Northern Beaches Council has submitted the statement to the IPC, Northern Beaches Council must:

- if practical, take reasonable steps to notify the contents of the statement to each of the individuals to whom the information relates; or
- if practical, take reasonable steps to notify contents of the statement to each of the individuals who are at risk from the eligible data breach.

If it is not practical to undertake either of the above, the Response Team must ensure a copy of the statement is published on Northern Beaches Council's website and reasonable steps are taken to publicise the contents of the statement (for example, by notifying its members).

Records Management

Documents created by the Response Team should be saved in the following folder:

C000199: CORPORATE MANAGEMENT - Policy - Administrative and Operational Policies for Common Administrative Functions - Privacy Management Plan and Privacy Matters - Information Management - Information and Digital Technology in CM10

CHECKLIST		
STEP 1 **Contain the breach and make a preliminary assessment**	☐	Convene a meeting of the data breach Response Team.
	☐	Immediately contain breach: o Take steps to contain the breach (will vary on a case-by-case basis) o Response Team to be alerted if necessary
	☐	Inform the CEO provide ongoing updates on key developments in the event of a serious breach
	☐	Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing Northern Beaches Council to take appropriate corrective action.
	☐	Consider developing a communications or media strategy to manage public expectations or media interest.
STEP 2 **Evaluate the risks for individuals associated with the breach**	☐	Conduct initial investigation, and collect information about the breach promptly, including: o the date, time, duration and location of the breach o the type of personal information involved in the breach o how the breach was discovered and by whom o the cause and extent of the breach o a list of the affected individuals, or possible affected individuals o the risk of serious harm to the affected individuals o the risk of other harms
	☐	Determine whether the content of the information is important.
	☐	Establish the cause and extent of the breach.
	☐	Assess priorities and risk based on what is known.
	☐	Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.
STEP 3 **Consider breach notification**	☐	Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
	☐	Determine whether to notify affected individuals – is there a *real risk of serious harm to the affected individuals?*
	☐	Consider whether others need to be notified, including police, Privacy Commissioner, or other agencies or organisations affected by the breach, or where [insert organisation name] is contractually required, or required under the terms of an MOU to notify specific parties.

STEP 4

Review the incident and take action to prevent future breaches

☐	Fully investigate the cause of the breach.
☐	Report to CET on outcomes and recommendations: ○ update security and response plan if necessary ○ make appropriate changes to policies and procedures if necessary ○ revise staff training practices if necessary ○ consider the option of an audit to ensure necessary outcomes are affected