Bayside Council
Serving Our Community

Data Breach Policy

22 November 2023

Data Breach Policy
File: F23/858 Document: 23/355124
Policy Register: F16/951 Policy No.: PP23/8
Class of document: Council Policy

Enquiries: Manager Governance & Risk

Contents

1 Introduction

1.1 Background

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 Council to notify the Privacy Commissioner and affected individuals of eligible data breaches and prepare and publish a Data Breach Policy (**DBP**) for managing such breaches.

1.2 What is an eligible data breach?

An 'eligible data breach' occurs where:

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.

Breaches can occur between agencies, within an agency and external to an agency.

The MNDB scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act, meaning information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

The scheme also applies to 'health information,' defined in section 6 of the *Health Records and* Information *Privacy Act 2002* (**HRIP Act**), covering personal information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

The scheme does not apply to data breaches that do not involve personal information or health information, or to breaches that are not likely to result in serious harm to an individual. Where the scheme does not apply, agencies are not required to notify individuals or the Commissioner but should still take action to respond to the breach. Agencies may still provide voluntary notification to individuals where appropriate.

1.3 Definitions

The definitions of certain terms are:

Data breach
an incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Bayside Council.

Personal information
information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Health information
A specific type of Personal Information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results.

Confidential information
Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, Security Classified Information and information related to the City's IT/cyber security systems.

1.4 Policy statement

Depending on the size and nature of a data breach, the consequences for individuals can be significant. They can give rise to a range of actual or potential harm to individuals. These consequences can include financial fraud, identity theft, damage to reputation and even violence.

Data breaches can also have serious consequences for Council. A breach may create risk through the disclosure of sensitive information, or otherwise impact an agency's reputation, finances, interests, or operations. Ultimately, data breaches can lead to a loss of trust and confidence in an agency and the services it provides.

Responding quickly when a breach occurs can substantially reduce its impact on affected individuals, reduce the costs to councils of dealing with a breach, and reduce the potential reputational damage that can result.

For these reasons, it is important that councils have a documented and operationalised plan or framework for quickly and effectively responding to and managing data breaches.

1.5 Scope of policy

The DBP outlines Council's overall strategy for managing data breaches from start to finish. Having a clear and well-defined DBP enables Council to:

- prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion
- mitigate potential harm to affected individuals and the agency itself
- meet compliance obligations under the PIP Act.

The DBP includes:

- how Council has prepared for a data breach
- a clear description of what constitutes a breach
- Council's strategy for containing, assessing, and managing eligible data breaches
- roles and responsibilities of Council staff members
- record keeping requirements
- post-breach review and evaluation

A concise description regarding such matters as:

- to whom the policy applies
- to what aspects of Council's business it applies.

2 Preparing for and managing data breaches

2.1 Data breach preparation

Council has the following processes in place to assist in preventing data breaches:

- Appropriate recruitment selection screening.
- Ongoing staff training and cyber security skills development.
- Appropriate supervisory and oversight arrangements for staff in key positions including separation of roles where appropriate.
- Periodic reviews of system access and removal of access no longer required due to job change.
- System design activities that consider the possibility of a data breach and implement appropriate mitigations (including externally provided IT services).
- Appropriate physical security of Council facilities that contain personal information.
- Preventative maintenance programs to address cyber security vulnerabilities which may expose personal information.
- Periodic IT security assurance assessments conducted by third parties at arms-length to Council.
- Cyber security forming a standing item to the IT Steering Committee.

2.2 Training and awareness

Most data breaches, both in Australia and internationally, involve a human element (e.g., either through direct human error or cyber-attacks that rely on a human compromise). Building a well- trained and aware workforce is a strong front-line defence against breaches and other privacy risks.

With respect to staff training and awareness Council will:

- enhance staff awareness of privacy and cyber principles and current threat trends by providing training and awareness around identifying, responding to and managing data breaches.
- schedule cyber security training for staff upon commencement and annual refresher training.
- share relevant examples of data breaches with staff, where appropriate.

2.3 Processes for identifying and reporting breaches

The quicker Council can detect a data breach, the better the chance that it may be contained, and potential harms mitigated through prompt action.

In order to identify data breaches, Council conducts audits and reviews, staff training and awareness and has technical controls for monitoring cyber security incidents that may lead to a data breach.

Council recognises that publishing these specific controls could create an additional risk for Council and, as such, only high-level processes are published in this document.

2.4 Appropriate provisions in contracts / other collaborations

Councils are often required to outsource functions to external service providers or another agency (for example, for IT solutions). These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements. To ensure agencies meet their obligations under the PPIP Act, these agreements often include provisions in relation to the management and notification of data breaches.

Council's approach to managing these collaborations and the contractual controls in place for ensuring external stakeholders comply with relevant privacy requirements are via contract provisions and not sharing personal information with third parties via email or other unsecured means.

2.5 Schedule for testing and updating the DBP

A DBP will only be effective if it is current, appropriately targeted and operationalised. As both the external threat environment, and Councils' internal makeup and functions, are continuously developing and changing, a DBP should be regularly reviewed to ensure it remains fit for purpose.

Regular testing of the data breach response process is the best way to ensure that all relevant staff understand their roles and responsibilities, and to check that the details of the response process (contact numbers, reporting lines, approval processes, etc.) are up to date. Testing the DBP could involve the development of a hypothetical or test incident and a review of the way agency personnel manage the event.

3 What a data breach is and how to identify one

Examples of data breaches that might occur in Council's context are:

- A cyber-attack resulting in potential or actual access or extraction of personal information (e.g. a malicious actor manipulates a Council online service to access other resident accounts either individually or in bulk)
- The loss of a Council owned device containing personal information and the potential or actual access or extraction of personal information contained within (e.g. a laptop containing locally stored email messages relating to residents or employees)
- The unauthorised distribution of personal information through methods such as email or file sharing services, including both malicious or accidental actions (e.g. the accidental emailing of a spreadsheet with payroll and bank account details, or the deliberate downloading of resident documents to a personal email account)

- The access or extraction of personal information for unauthorised purposes by those trusted with access to that information. (e.g. a staff member looking up an ex-partner's personal details to find their home address or contact details).

In a Council context, personal information could include, but is not limited to:

- Employee personal information including prospective, current, and former employees. This could include tax file numbers, bank and salary information, home addresses, next of kin and medical related records.
- Customer information including residents, ratepayers and users of Council facilities and services. This could include bank accounts, home addresses, email addresses, service usage information and mobile phone numbers.
- Councillor information including prospective, current and former councillors. This could include home addresses, bank accounts and financial information.
- CCTV information including the capture, storage and dissemination of images of persons.
- Motor Vehicle information in connection with enforcement of local laws including vehicle owner personal information.

Serious impacts of a data breach could include:

- Risk to individuals' safety
- Risk of identity theft
- Financial loss to an individual or organisation
- Damage to personal reputation or position
- Humiliation, embarrassment or bullying
- Damage to reputation.

4 Reporting and responding to data breaches

4.1 Plan to triage, contain, assess, notify, prevent

Contain the breach and conduct a preliminary assessment

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 lead to the breach, 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 advice from Cyber Security NSW, legal advice 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.

Where practicable, we will preserve all relevant evidence to assist with assessment of the extent of the breach and to enable investigation (including by law enforcement agencies, if necessary).

Evaluate and mitigate the risks associated with the breach

Remedial action should be taken as soon as practicable, to prevent or lessen the likelihood that the breach will result in harm to any individual.

Consider what staff should be told about the breach, to help contain the breach and prevent further breaches such as not clicking on emails with attachments and being aware of phishing attacks. Messaging should include that staff must not comment publicly or privately (including on social media), that any media communications must be handled by the Manager Communications and Events and that all other enquiries must be referred to the Manager Governance (as Council's Privacy Officer).

The Manager Communications and Events will provide advice to the Manager Customer Experience about handling enquiries from customers. Complete an assessment to determine whether there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in, serious harm to one or more individuals to whom the information relates.

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 Council 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 the Council's reputation?
- **Guidance issued by the Privacy Commissioner on assessing eligible data breaches** Upon becoming aware of a possible data breach, the Council will take into account any guidance issued by the NSW Privacy Commissioner.

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken. Some types of data are more likely to cause harm if compromised. 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).

4.2 Strategies for managing supplier and/or partner agency breaches

Detailed strategies for managing data breaches that may occur at business-critical suppliers or partners that affect agency data are included in Bayside's Data Breach Response Plan.

4.3 Other obligations including external engagement or reporting

The 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 Council suspects a data breach is a result of criminal activity.
- 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.

4.4 Clear communication strategy

Notify and communicate

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:

- Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.
- 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, the Council may not be required to notify affected individuals.
- Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
- Provide further information to the Privacy Commissioner.

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 business days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, the 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 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 Council's 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.

4.5 Capability, expertise, and resourcing

Constitute a Data Breach Response Team:

A Data Breach Response (DBR) Team will be constituted in the following circumstances:

> If more than 1 individual is affected by a data breach and it has been determined by the Manager Governance & Risk or the Chief Information Officer that the breach could result in serious harm and the notification provisions of this policy are triggered and the breach has not been contained.

The DBR Team should include:

- the Manager Governance & Risk (Privacy Officer)
- General Manager
- Chief Information Officer
- Manager Customer Experience
- the custodian of the data affected by the breach

- the manager of the business area where the data breach occurred
- Manager Communications & Events (if required).

If a contracted service provider or other agency is involved in the data breach, create a Joint Response Team.

5 Policy implementation

5.1 Roles and responsibilities

General Manager

- Ensure Council has systems in place to comply with the MNDB Scheme.
- Review and approve actions and recommendations in data breach reports.
- Demonstrate to the affected individuals and broader public that Bayside Council views the protection of personal information as an important and serious matter.

Manager Governance & Risk (Privacy Officer)

- On being alerted to a data breach immediately notify the General Manager and the Chief Information Officer.
- Review proposed actions and recommendations in reports prepared by the Chief Information Officer and provide to the General Manager for approval.
- If the breach relates to any area other than Information Technology or Information Management, investigate the breach in a timely and effective manner and prepare a report to provide to the General Manager for approval.
- Implementation of proposed actions and recommendations, including any follow up with otherstaff.
- Notify the Privacy Commissioner if the breach results (or could result) in serious harm to an individual(s) or if the data breach resulted in personal information being disclosed and there arerisks to the privacy of individuals. This could include notification to external stakeholders or other bodies.
- Constitute a Data Breach Response Team, if required (see further details below).

Chief Information Officer

- If the breach relates to Information Technology or Information Management, investigate the breach in a timely and effective manner and prepare a report to provide to the Manager Governance & Risk, who will review the proposed actions and recommendations of the report and provide to the General Manager for approval.
- If the breach relates to Information Technology or Information Management, implement any proposed actions and recommendations, and keep the Manager Governance & Risk informed of progress.

Manager Communications & Events

- Coordinate the messaging to the public and communication to individuals affected by data breaches with referral to the Data Breach Response Team.

Manager Business Transformation

- Coordinate and deliver staff training and awareness

Data Breach Response Team

- Review the Manager Governance & Risk and/or Chief Information Officer's initial assessment of the data breach.
- Establish roles within the team based on subject matter expertise (which could include incidentresponse specialists, legal, communications, cybersecurity, physical security, human resources, key agency operations staff, key outsourcing/relationship managers).
- Delineation of responsibility for dealing with relevant elements of a breach within the team.
- Investigate the breach using the process in line with this policy.
- Make recommendations regarding Council's Business Continuity Plan, particularly if ITsystems must be shut down.
- Participate in the post data breach review.

Staff

It is everyone's responsibility to be aware of this Plan and to report suspected data breaches as soon as possible.

Even if you have contained the breach (for example, retrieved a stolen laptop or lost hard-copy files), you must still tell the Manager Governance & Risk. The Manager Governance & Risk will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.

5.2 Record keeping

Appropriate records must be maintained to provide evidence of how suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner.

Tracking data breaches allows us to monitor, analyse and review the type and severity of suspected breaches along with the effectiveness of the response methods. This may help to identify and remedy weaknesses in security or processes that are prone to error.

Council will meet its record keeping obligations under the PPIP Act by:

- Maintaining and publishing (on our website) a public notification register for any notifications given under section 59N(2).
- Establishing and maintaining an internal register for eligible data breaches.
- Publishing our Privacy Management Plan and DBP on our website.

Eligible Data Breach Incident register – Council will establish and maintain an internal register for eligible data breaches. Each eligible data breach must be entered on the register, with the following information included for each entry where practicable:

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

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

5.3 Post-breach review and evaluation

The 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. 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.

5.4 Procedures

Procedures that support this policy, may be approved by the General Manager from time to time and address such issues as:

- administrative workflow for approvals

6 Document control

6.1 Review

This policy will be reviewed every two years or as required by best practice or legislation changes.

6.2 Related documents

- Government Information (Public Access) Act 2009
- NSW IPC Guide to preparing a data breach policy
- NSW IPC Guide to managing data breaches in accordance with the PPIP Act
- Health Records and Information Privacy Act 2002
- Privacy and Personal Information Protection Act 1998
- Bayside Council Privacy Management Plan.
- Bayside Council Cyber Incident Response Plan

6.3 Version history

Version	Release Date	Author	Reason for Change
1.0	22/11/2023 (Council)	Coordinator Governance	New document