


STRATHFIELD COUNCIL

DATA BREACH POLICY

10 October 2023



	<h2>DATA BREACH POLICY</h2>		
RESPONSIBILITY	Manager Governance and Risk		
DATE ADOPTED	10 October 2023	MINUTE	253/23
REVISED		REVIEW	
CM10 No	23/60893		
ASSOCIATED POLICIES	Business Ethics Statement Code of Conduct Privacy Management Plan Records Management Policy		
ASSOCIATED LEGISLATION	<i>Privacy and Personal Information Protection Act 1998</i> <i>Health Records and Information Privacy Act 2002</i> <i>State Records Act 1998</i>		

1.0 Introduction

This policy sets out how Strathfield Council manages a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach.

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

This policy has been written in relation to Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) establishing the NSW Mandatory Notification of Data Breach (**MNDB**) scheme.

1.1 Title and Commencement

This policy is titled Data Breach Policy. This policy was adopted by Council resolution (253/23) after public exhibition from xx to xx.

1.2 Background and Purpose of Policy

A Data Breach can have significant consequences for individuals that can give rise to a range of actual or potential harm. These consequences can include financial fraud, identity theft, damage to reputation and even violence.

The purpose of this policy is to outline how Strathfield Council applies the MNDB Scheme which 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 MNDB scheme Strathfield Council has prepared a Data Breach Policy (DBP) for managing such breaches.

1.3 Objectives of the policy

The objectives of this policy are to:

- Respond quickly when a Data Breach occurs.
- Mitigate potential harm to affected individuals and the Council.
- Meet compliance obligations under the PPIP Act.

1.4 Coverage of the Policy

The policy applies to data that is held in physical or digital format that is defined as 'personal Information' under the PIPP Act Section (4).

1.5 Definitions

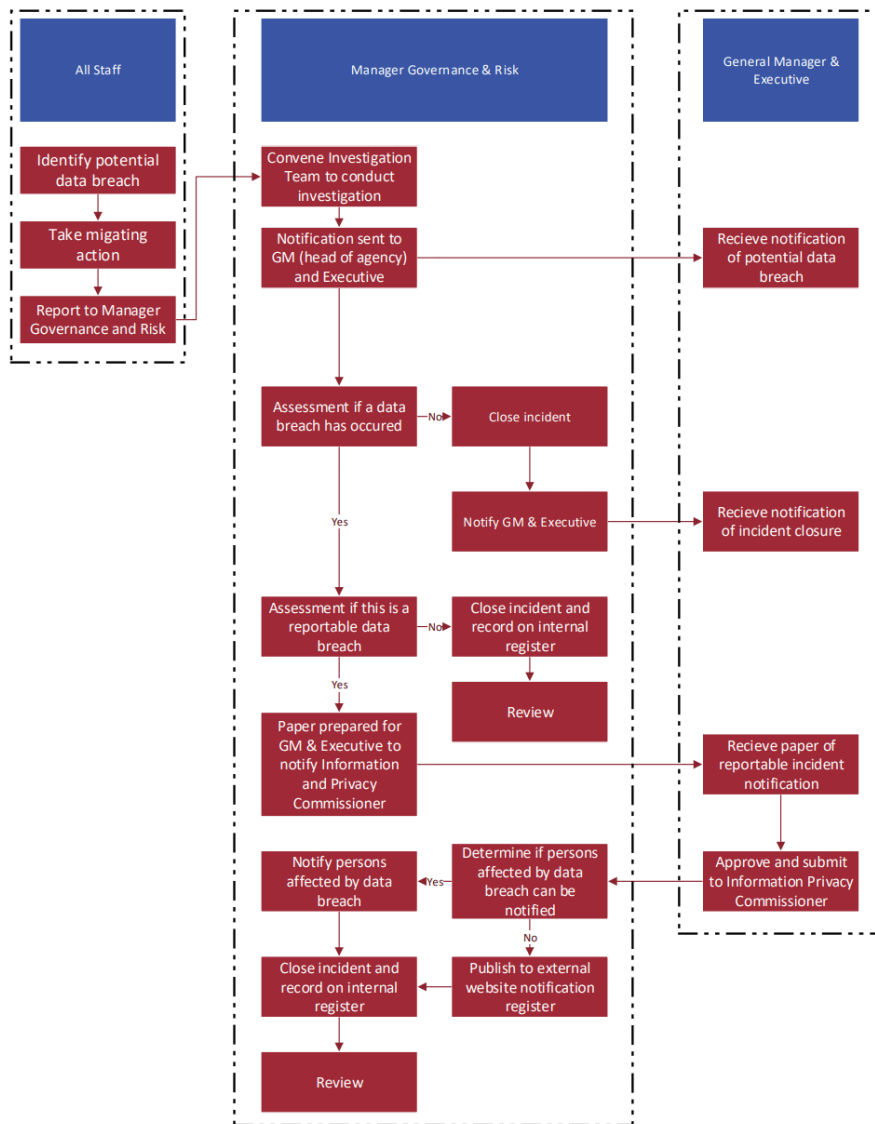
- **Data Breach** - For the purposes of this policy, a Data Breach occurs when there is a failure that has caused Unauthorised Access to, or disclosure of Confidential Information held by Strathfield Council.
- **Data Breach Investigation Team** – A core team of Council staff with responsibility for initiating review of a suspected Data Breach. Depending on the nature and circumstances of the breach, other employees may be called on to form part of the Data Breach Investigation Team.
- **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 Strathfield Council's IT/cyber security systems.
- **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.
- **Information** - including written text, images, videos, and audio recordings.
- **Personal Information** - Information or an opinion (including Information or an opinion forming part of a database and whether in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the Information or opinion. This includes, for example, their name, address, email address, phone number, date of birth or photographs.

- **Security Classified Information** - Information and data (including metadata) that is marked as Protected, Secret, or Top Secret as per the Commonwealth Attorney Generals' Department's Protective Security Policy Framework.
- **Unauthorised Access** - Examples include:
 - an employee browsing customer records without a legitimate purpose.
 - a computer network being compromised by an external attacker resulting in Personal Information being accessed without authority

2.0 Policy Statement

2.1 Roles and responsibilities of staff members.

Position	Role/function
General Manager	Head of Agency, Strathfield Council
Director Engineering and Operations	Executive Committee member
Director Corporate and Community	Executive Committee member
Director Environment and Planning	Executive Committee member
Manager Governance & Risk	Investigation Team coordinator
General Counsel	Investigation Team member
Manager Digital, Information & Customer	Investigation Team member
Manager People & Culture	Investigation Team member
Manager Communications & Events	Investigation Team communications advisor
ICT Infrastructure and Support Coordinator	Subject Matter Expert
Information Management Coordinator	Subject Matter Expert



All employees will:

- immediately report any actual or suspected Data Breaches to the Manager Governance & Risk.

The Manager Governance & Risk will:

- immediately notify the Data Breach Investigation Team and assemble the Team as soon as possible.
- undertake relevant internal notifications as required by this policy.

The Data Breach Investigation Team will:

- assemble promptly to review and respond to a Data Breach
- follow this policy when responding to a Data Breach
- consult with internal and external stakeholders as required.
- prepare a Data Breach review report for each separate Data Breach incident.

The Manager Digital, Information and Customer will:

- take immediate and any longer-term steps to contain and respond to security threats to the Strathfield Council's IT systems and infrastructure.

The Manager Risk and Governance will:

- undertake notifications as required to affected individuals/organisations and the NSW Privacy Commissioner
- notify the Strathfield Council's insurers as required.

Consultation

The following teams have been consulted in the development of this policy:

- Executive
- General Counsel
- Digital Information and Customer
- Governance and Risk
- People and Culture

2.2 What constitutes a breach and when to report.

A Data Breach occurs when Personal Information an organisation or agency holds is lost or subjected to Unauthorised access or disclosure. For example, when:

- a device with a customer's Personal Information is lost or stolen.
- a database with Personal Information is hacked.
- Personal Information is mistakenly given to the wrong person.

At any time, a Council officer is aware of a potential Data Breach this is to be reported to Manager Governance & Risk to initiate a preliminary assessment to determine if the circumstance warrants initiating protocols as outline in this Data Breach Policy and convening the Data Breach Investigation Team.

It is then up to the Data Breach Investigation Team coordinator to recommend to the General Manager whether the Data Breach is notifiable to the NSW Privacy Commissioner.

IPC Data breach case studies

Case study 1: Mail merge problem

A mail-merge problem at a large government Agency has resulted in emails being sent to the wrong recipients. The subject of the email was a retirement party being held for an outgoing employee and the email included details about the employee, the date and location of the party, and the contact details of the sender. After a brief look at the recipients list, it was seen that the email was accidentally sent to unintended internal business teams, as well as a few external consultants.

In this case, while information was sent to a reasonable number of unintended recipients, the consequences are limited to some potential embarrassment caused to the retiring employee and a minor level of reputational damage that may result from the external consultants identifying that a mistake has been made. This would not constitute a serious breach and should be handled internally. Reporting to the Privacy Commissioner is not recommended in this case. Actions may include apologies being sent out and the mail merge problem being addressed.

Case study 2: Lost laptop

The daughter of staff member at a smaller regional council had her laptop computer stolen at a university library. Upon hearing about this, the staff member remembered having used the daughter's laptop during a conference and suspected that the laptop still had copies of unsecured spreadsheets containing sensitive information on the computer's desktop. This information included account access, financial and personal information about council staff. The daughter was not sure whether the laptop was password protected. In the hope of recovering the laptop, the staff member waited until the police investigation was over before reporting the breach to management.

This would be considered a serious breach and should have been reported to the council immediately and then in turn to the Privacy Commissioner. A combination of factors, including the fact that the laptop is a personal device and unable to be monitored or secured by council IT staff, the sensitive nature of the information that has been compromised and its potential for misuse, and the uncertainty around the security setting on the laptop itself, and the long length of time between when the breach occurred and when it was identified by the council, all contribute to the likelihood that serious harm could occur. The lack of immediate notification to the council means that steps to potentially isolate and mitigate damage could not have been taken. The Privacy Commissioner's assessment would look at the details of the breach, the actions taken in response to the breach, and would potentially suggest improvements to staff training, device-use policies and data breach response plans.

2.3 How Strathfield Council has prepared for a Data Breach.

Strathfield Council's Manager of Governance and Risk or nominee of the General Manager must be informed of any Data Breach to ensure the application of this policy. Subsequently advice is provided to the General Manager to assist in responding to enquiries made by the public, and managing any complaints that may be received as a result of the breach.

There are four key steps required in responding to a Data Breach:

1. Containing the breach or suspected breach
2. Assessing or evaluating the Information involved in the breach and the associated risks
3. Notifying affected individuals / organisations affected by the breach
4. Preventing a repeat with post incident review and preventative efforts

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Manager Digital, Information and Customer provides support with the supply and maintenance of its IT systems. The Manager of Governance and Risk or General Manager nominee will coordinate with the Manager Digital, Information and Customer and/or 3rd party service providers to address and respond to identified Data Breaches related to its IT systems.

2.3.0 Initial Assessment and Triage of Breach Reports.

Reports of potential Data Breaches will be submitted with the following information to guide the initial assessment and triage of such reports.

- When and where did the breach occur
- Estimated number of individuals affected.
- Description of immediate actions taken to contain the data breach.
- Was anyone else notified of the data breach? (i.e. health service, NSW Police etc.)
- Cause and estimated cost of the data breach (if known).
- Has evidence been preserved? Please specify.
- Severity Rating

2.3.1 Containing the breach or suspected breach.

Containing the breach is prioritised by Strathfield 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, 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 Strathfield Council to seek legal or other advice on what action can be taken to recover the data. When recovering data, Strathfield Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

2.3.2 Assessing or evaluating the Information involved in the breach and the associated risks.

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 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 Strathfield Council's 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? Strathfield 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? Strathfield Council assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. 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? Strathfield Council's 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 Strathfield Council's reputation?

2.3.3 Notifying affected individuals / organisations affected by the breach.

Strathfield Council recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations.

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

Strathfield Council will have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, Information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and desensitise individuals to a significant privacy breach.

Factors Strathfield Council will consider when deciding whether notification is appropriate include:

- Are there any applicable legislative provisions or contractual obligations that require Strathfield Council to notify affected individuals?
- What type of Information is involved?
- What is the risk of harm to the individual/organisation?
- Is this a repeated and/or systemic issue?
- What risks are presented by the mode of the breach e.g. is it encrypted Information or contained in a less secure platform e.g. email?
- What steps has Strathfield Council taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if the individual/organisation would not be able to take steps to rectify the situation, is the Information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

Notification should be done promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

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

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as Information posted on Strathfield 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 are 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).

What to say

The notification advice will be tailored to the circumstances of the breach.

Content of a notification could include:

- Information about the breach, including when it happened.
- a description of what data or Personal Information has been disclosed.
- assurances (as appropriate) about what data has not been disclosed.
- what Strathfield Council is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what Strathfield Council will do to assist people with this?
- contact details for Strathfield Council for questions or requests for Information.
- the right to lodge a privacy complaint with the Privacy Commissioner

2.3.4 Preventing a repeat with post incident review and preventative efforts.

Strathfield 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:
 - security audit of both physical and technical security controls
 - review of policies and procedures
 - review of staff/contractor training practices; or
 - review of contractual obligations with contracted service providers.

Preventive measures include:

- Cyber Security Training and Awareness
- Monitoring
- Privacy Awareness Training
- Internal Communications (email newsletter)
- Risk Management Framework
- Securing and Digitising Paper Records

2.4 Notifying the Privacy Commissioner

When a Data Breach has been classified as reportable i.e., where Personal Information has been disclosed and there are risks to the privacy of individuals, the Manager of Governance and Risk will advise the General Manager of the requirement to notify the NSW Privacy Commissioner of a Data Breach using the approved IPC Mandatory Data Breach Reporting Form.

In doing so Strathfield Council will ensure that relevant evidence is contained securely for access by the Privacy Commissioner should regulatory action be considered appropriate. Such notification will:

- demonstrate to the affected individuals and broader public that Strathfield Council views the protection of Personal Information as an important and serious matter and may therefore maintain public confidence in Strathfield Council
- facilitate full, timely and effective handling of any complaints made to the Privacy Commissioner regarding the breach and thus assist those whose privacy has been breached.

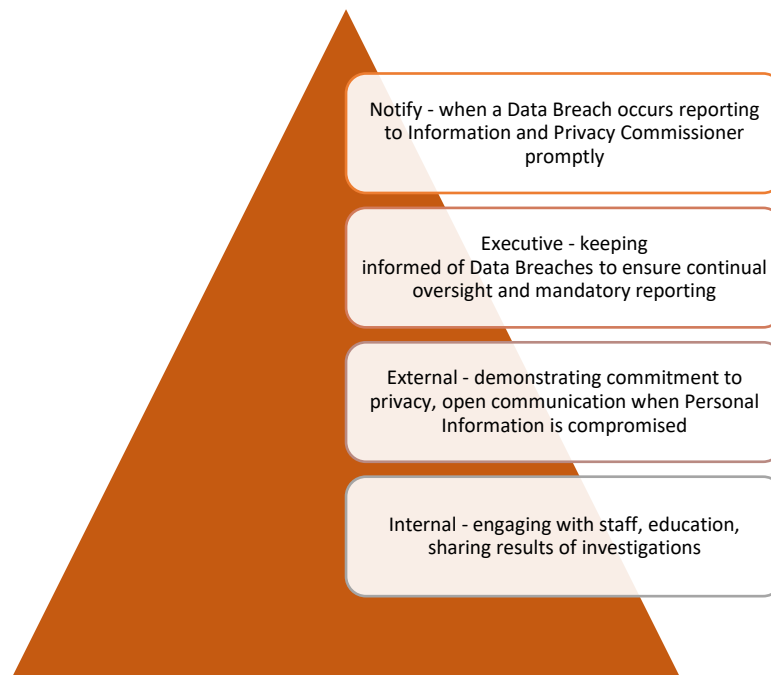
Notification should contain similar content to that provided to individuals/organisations. The Personal Information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach
- the type of Personal Information involved in the breach.
- what response Strathfield Council has made to the breach?
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person, and
- whether the breach has been notified to other external contact(s).

External stakeholders

- NSW Police Force
- Department of Customer Service
- Cyber Security NSW
- The Office of the Australian Information Commissioner
- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- Any third-party organisations or agencies whose data may be affected.
- Financial services providers
- Professional associations, regulatory bodies or insurers

Communication



2.5 Record keeping requirements.

Internal incident Register – Stored in record management system

Who was notified of the breach	When the breach was notified	The type of breach	Details of steps taken to mitigate harm	Details of actions to prevent future breaches	Estimated cost of breach	Severity

an agency is required under section 59ZE to establish and maintain an internal register of eligible Data Breaches. This register should record the Information specified under section 59ZE(2).

Number of people potentially affected	Date of breach	Description of breach	Type of breach	How the breach occurred	Type of Personal Information impacted
Actions taken to mitigate harm	Recommended steps for individuals in response to breach	Date of notice publication	Contact for further Information	Link to full public notification	Actions taken to mitigate harm

Public notification Register –published on website

agencies are required to maintain a public notification register of any notifications made under section 59N(2). The Information recorded in the register must be publicly available for at least 12 months after the date of publication and include the Information specified under section 59O.

3.0 Version Control

Date	Type	Minute
10/10/2023	Adoption	253/23