CORPORATE SERVICES

Data Breach Policy

Adoption Date:
24 October 2023

Review Date:
24 October 2025

Version:
1

Responsible Department:
Customer & Compliance

TRIM Document Number:
D04997254

Randwick City Council
a sense of community

Contents

Version	Adoption date	Comments
1	24 October 2023 Council meeting	New policy

This policy will be reviewed every two years or as required as best practice, legislation or government polices change.

Introduction

Part 6A of the Privacy and Personal Information Protection Act 1998 (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.

1. Scope

This policy applies to all Councillors, staff and contractors of Randwick City Council. This includes temporary and casual staff, private contractors and consultants engaged by the Council to perform the role of a public official.

2. Purpose

The purpose of this policy is to provide guidance to Randwick City Council staff in responding to a breach of Council held data, especially personal information. This policy sets out Council's response plan for managing 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 Council in avoiding or reducing possible harm to both the affected individuals/organisations and Council, and may prevent future breaches.

3. What is an eligible data breach?

An eligible data breach occurs when:

1. there is unauthorised access to, or unauthorised disclosure of, personal information held by Council or there is a loss of personal information held by Council 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.

Data breach means:

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

The MNDB scheme applies to breaches of 'personal information' as defined in the PPIP Act.

Personal information means:

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

Note: The scheme also applies to 'health information,' defined in the Health Records and Information Privacy Act 2002 (HRIP Act).

A data breach may be deliberate or accidental and may occur by a range of different means or channels, including but not limited to, loss or theft of physical devices, misconfiguration or over-provisioning of access to sensitive systems, inadvertent disclosure, social engineering or hacking.

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 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).

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, Council is not required to notify individuals or the Information and Privacy Commission (IPC) but will still take action to respond to the breach. Council may still provide voluntary notification to the IPC and individuals where appropriate.

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

- Employee 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.

3.1. Tax File Numbers

Although NSW public sector agencies are exempt from most of the federal *Privacy Act 1988 (Cth)*, the data breach notification requirements in relation to Tax File Numbers (TFNs) apply.

All organisations which receive TFNs, whether from new employees or in other circumstances, must comply with the *Privacy (Tax File Number) Rule 2015* (the TFN Rule). The TFN Rule is issued under section 17 of the federal *Privacy Act*, and sets out requirements for the collection, use, disclosure, data security and disposal of individuals' TFN information.

A breach of the TFN Rule is considered an eligible data breach, and thus an organisation which experiences a data breach involving TFNs must comply with the mandatory notifiable data breach scheme under the federal *Privacy Act*. This involves notification to the affected individuals, and to the Australian Privacy Commissioner.

3.2. What is serious harm?

Likely to result in serious harm means:

'Serious harm' includes such things as serious physical, psychological, emotional, financial, or reputational harm.

'Likely' means the risk of serious harm to an individual is more probable than not.

Breaches of personal data can result in significant harm, including people having their identities stolen or the private home addresses of protected or vulnerable people being disclosed. In some circumstances, this can expose an individual to a significant risk of harm. As such, even a breach affecting a small number of people may have a large impact.

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.

For further information in relation to assessing the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure, refer to Section 7.3.1 of this policy.

4. Quick decision tree guide

Has personal (or health) information been lost, or subject to unauthorised access or disclosure?	
If YES – Report the data breach to the Privacy Officer (Manager Customer & Compliance) immediately	If NO – Report other cyber security incidents to the Manager IM&T immediately
Is the breach likely to result in serious harm?	
If YES – report the data breach to the General Manager immediately	If NO – the Privacy Officer (Manager Customer & Compliance) will manage the process from here; assist the Privacy Officer as requested

5. How we have prepared for a data breach

5.1. 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.

5.2. Processes in place for preventing data breaches

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 Audit, Risk and Improvement Committee.

5.3. Processes in place for identifying data breaches

Council has the following processes in place for identifying data breaches:

- Technical controls, such as Data Loss Prevention tools, USB monitoring and antivirus systems.
- Monitoring services, including services provided by Cyber Security NSW for Council to monitor for data and credentials that may appear on the dark web.
- Audits and reviews
- Staff training and awareness.

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.

6. Roles and responsibilities of staff members

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 Randwick City Council views the protection of personal information as an important and serious matter.

Manager Customer & Compliance (Privacy Officer)

- On being alerted to a data breach immediately notify the General Manager and the Manager IM&T.
- Review proposed actions and recommendations in reports prepared by the Manager IM&T 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 using the template at Appendix A and provide to the General Manager for approval.
- Implementation of proposed actions and recommendations, including any follow up with other staff.
- 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 are risks to the privacy of individuals. This could include notification to external stakeholders or other bodies.
- Constitute the Data Breach Response Team, if required (see further details below)

Manager IM&T

- If the breach relates to Information Technology or Information Management, investigate the breach in a timely and effective manner and prepare a report using the template at Appendix A and provide to the Manager Customer & Compliance, 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 Customer & Compliance informed of progress.

Manager Communications

- Authorise communication to individuals affected by data breaches. See template response at Appendix B and section 7.3.3 of this policy “Notify & Communicate” – “what to say”.

Data Breach Response Team

- Review the Manager Customer & Compliance’s and/or Manager IM&T’s initial assessment of the data breach
- Establish roles within the team based on subject matter expertise (which could include incident response 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 four step process outline in this policy.

- Determine whether Council's Business Continuity Plan needs to be invoked, particularly if IT systems have to be shut down.

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 Privacy Officer. The Privacy Officer will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.

7. Responding to a data breach

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

7.1. How to report

In all cases, you must report a suspected data breach immediately, either in person or by phone call, to the Privacy Officer:

> **Manager Customer & Compliance (David Kelly) – phone 9093 6742 or 0410438680 or by email david.kelly@randwick.nsw.gov.au.**

Report in person or by phone and then confirm your report in writing, by email.

The Manager Customer & Compliance will notify the Manager IM&T (as the manager responsible for both information management and information technology).

If the Manager Customer & Compliance **or** the Manager IM&T believe the suspected data breach is likely to result in serious harm to any individual, they must report it immediately to the General Manager.

7.2. Overview of procedure for the Privacy Officer

Depending on the nature of the breach, the law might consider it a 'notifiable data breach', meaning that the affected individuals and the appropriate regulator ***must*** be notified. The Manager Customer & Compliance (in conjunction with the Manager IM&T, if required) will make an assessment about this, in accordance with the Data Breach Response Procedure outlined below.

<table>
<tr><td colspan="3">Step 1: Contain the breach</td></tr>
<tr><td colspan="3">Step 2: Assess the breach:
- Is the breach likely to result in serious harm to individuals?
- Does the breach involve TFNs?</td></tr>
<tr><td>If YES – Step 3: Evaluate, mitigate and notify</td><td>If UNCLEAR – Assess within 30 days to determine whether Yes or No</td><td>If NO – Optional: Evaluate, mitigate and notify</td></tr>
<tr><td>Mandatory notification: Notify the IPC (or relevant privacy regulator) as soon as practicable</td><td></td><td>Voluntary notification to the IPC</td></tr>
<tr><td></td><td>Notify the affected individuals as soon as practicable</td><td></td></tr>
<tr><td colspan="3">Step 4: review and report</td></tr>
</table>

7.3. Strategies for managing and responding to data breaches

Council will utilise a four-step process when responding to data breaches. It is the responsibility of the Manager Customer & Compliance (Privacy Officer) to manage this process, ensure it is completed and document the steps taken. Appendix A to this Plan provides a standard format for reporting.

Any enquiries received about any data breach should be directed to the Manager Customer & Compliance (Privacy Officer) in the first instance.

7.3.1. Step 1: 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).

- **Take all realistic steps to contain the breach:**

This may involve searching for and recovering the data, confirming that no copies were made or that the information was destroyed by the party receiving it, a remote wipe has been done on a lost portable device, computer system shut down, or passwords and system usernames have been changed.

- **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 Customer & Compliance or the Manager IM&T 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 Customer & Compliance (Privacy Officer), General Manager, Manager IM&T, the custodian of the data affected by the breach, the manager of the business area where the data breach occurred, Leader Enterprise Risk & Safety (if required), Manager Communications (if required). If a contracted service provider or other agency is involved in the data breach, create a Joint Response Team.

- **Conduct preliminary fact-finding about the breach, including type of data (e.g. check if TFNs were involved), cause, risk of spread and options to mitigate.**
- **Make a preliminary assessment of the risk posed by the breach, as Low, Medium or High, according to the criteria below. Document this decision using the Response Report in Appendix A to this Plan.**

Risk Assessment	
Low risk data breach means:	A loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur (e.g. paper files are left behind in a meeting but quickly retrieved).
Medium risk data breach means:	A loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent, and that the data is somewhat protected (e.g. a laptop with encrypted data is left on a bus).
High risk data breach means:	It is reasonably believed that the data breach is ***likely to result in serious harm*** to one or more of the individuals to whom the information relates (e.g. external hackers breach our firewall and copy valuable customer data).

- **Consider who else needs to be informed about the breach, and/or involved in the Response Team, depending on the risk level:**
    - Low risk: INFORM -
        - Leader Enterprise Risk & Safety
        - custodian of the data affected by the breach
        - manager of the business area where the data breach occurred
    - Medium risk: INFORM -
        - General Manager's Team (GMT)
        - Leader Enterprise Risk & Safety
        - Manager IM&T Services if the data breach involved a failure or compromise of data security
        - custodian of the data affected by the breach
        - manager of the business area where the data breach occurred
        - Manager Communications (if required)
    - High risk: INFORM -
        - General Manager and/or General Manager's Team (GMT)
        - Leader Enterprise Risk & Safety
        - Manager IM&T Services if the data breach involved a failure or compromise of data security
        - Coordinator Customer Service
        - Manager Communications
        - custodian of the data affected by the breach
        - manager of the business area where the data breach occurred
        - the Council
        - Audit, Risk & Improvement Committee (ARIC)
        - Council's Insurer (via the Leader Enterprise Risk & Safety)
        - Council's Solicitors (if required)
        - NSW Privacy Commissioner
- Consider whether to involve any other external parties at this stage.

  If the breach involves cybercrime, contact the Australian Cybercrime Online Reporting Network which will coordinate a police response.

  For other types of criminal activity (eg. theft), contact the local police.

  For other cybersecurity incidents requiring support or assistance, contact Cyber Security NSW.
- Avoid destroying any evidence that may be necessary to investigate the breach, if at all possible.
- Log the incident in the relevant Risk Incident Register (contact the Leader Enterprise Risk & Safety) and monitor and report to the General Manager regularly until the threat has been eliminated.

7.3.2. Step 2: Evaluate and mitigate the risks associated with the breach

- Take remedial action 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 that all other enquiries must be referred to the Manager Customer & Compliance (as Council's Privacy Officer).
- Work with the Manager Communications to provide advice to the Coordinator Customer Service about handling enquiries from customers. A set of prepared FAQs can assist.
- Complete an assessment:
    - The assessment must 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 of the individuals to whom the information relates.

- This assessment must be completed **as soon as practicable**, and at the very latest within 30 calendar days. **Ideally, the assessment should be done within 2-3 days**. The assessment must be documented using the Response Report in Appendix A to this Plan.
- Note **it may be necessary to commence Step 3** (Notification) before the assessment has been completed or the breach fully contained.

- Engage appropriate expertise to help you or the Response Team conduct the assessment and evaluate/mitigate any risks. In addition to the people already involved, consider involving for example forensic investigators, risk advisers, and any outsourced service providers which store, use or otherwise handle personal information, or could be affected by the breach.
- The **assessment** about the **likelihood of serious harm** should have regard to:
  - the type of information involved: e.g. was it name and address, financial information, health records, evidence of identity documents or other unique identifiers or types of 'sensitive information': information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership
  - the volume of information involved: was it a combination of pieces of data about the individual which would not otherwise be known?
  - whether the information is protected by one or more security measures – e.g. what is the likelihood that any of the security measures could be overcome?
  - the risk profile of the information involved: e.g. could it be used for identity theft or other fraudulent purposes? to humiliate or blackmail the individual? to commit physical harm?
  - the type of individuals affected: are the individuals particularly vulnerable (e.g. victims of family violence), or is the information particularly valuable because the individuals involved are worth targeting in some way, such as very wealthy people, celebrities, public figures, or notorious individuals?
  - how much time passed between becoming aware of the data breach and containing it?
  - the context: was this an isolated incident, a systemic problem, a deliberate attempt to steal data, or the result of an accident or other unintentional behaviour?
  - how likely is it, that the persons who may have obtained the information have an intention to cause harm to any of the individuals affected by the data breach?
  - the further effects: is there a risk of ongoing breaches or further exposure of the information?
  - the risk of harm to affected individuals, as well as to other stakeholders: have there been breaches in other agencies that could result in a cumulative effect of more serious harm?
  - the extent to which the risk has been successfully prevented or lessened by any remedial action or containment efforts: e.g. was the data encrypted, was the portable storage device remotely wiped, were the hard copy files quickly recovered?
  - given all of the above, the type of harm likely to affect the individuals: e.g. identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of job opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalisation.

Note that the number of individuals affected is not directly relevant to this particular assessment. **Our legal notification obligations can be triggered even if only one person is likely to suffer serious harm**. However, our response plan will be shaped by the number of individuals who are affected.

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). Factors to consider include:

- **Who is affected by the breach?**

Council's 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?**

Council's 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?**

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 or 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? Does it risk embarrassment or harm to an individual(s).

7.3.3. Step 3: Notify and communicate

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. Accordingly, Council adopts a relatively low threshold in considering whether to notify individuals of the release or risk to the security of their personal information and will generally make such a notification.

Council will also 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 de-sensitise individuals to a significant privacy breach.

- **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.

Consider the option to postpone disclosure and/or notification if a security organisation (e.g. Cyber Security NSW or the Australian Cyber Security Centre) requests this in the circumstances (examples could include; if an event is deemed cyber terrorism etc).

- **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 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 particular 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 Council is doing to control or reduce the harm

- what steps the person/organisation can take to further protect themselves and what Council will do to assist people with this
- contact details for a Council officer for questions or requests for information
- the right to lodge a privacy complaint with the Privacy Commissioner.

- As soon as the assessment at Step 2 has been completed, our legal notification obligations are triggered.
- Notification is required by law if TFNs were involved and the assessment has concluded that 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 of the individuals to whom the information relates (ie. a High Risk breach). In relation to a data breach involving TFNs, the statement **must be sent to the Australian Privacy Commissioner** (part of the Office of the Australian Information Commissioner, or OAIC) **as soon as practicable**. The OAIC has an electronic form for reporting data breaches. The Response Report in Appendix A to this Plan contains the information needed to complete the OAIC's electronic form. The OAIC can also be contacted via email to enquiries@oaic.gov.au, or by telephone on 1300 363 992.
- Notification is also required by law if the data involved was received from another agency and we have become aware that privacy legislation has been (or is likely to have been) breached in relation to that data, while the data was in Randwick City Council's control; in such a case, our mandatory obligation is to inform the data provider and the NSW Privacy Commissioner, while informing any affected individuals is voluntary.
- Notification is voluntary in all other cases (ie. Low Risk and other Medium Risk breaches). Consider the reasonable expectations of the individuals concerned, as well as our reputation if we do or don't notify. If we choose to *voluntarily* notify affected individuals, we do not need to notify the regulator, though it is best practice to do so nonetheless.
- Mandatory notification requires the Manager Customer & Compliance (Privacy Officer) to:
    - Prepare a statement as soon as practicable. The statement must set out:
        - the name and contact details of this agency
        - a description of the data breach
        - the kind(s) of information concerned
        - describe the action being taken to rectify the breach and mitigate any harm
        - recommendations about the steps that individuals should take in response (eg. link to www.idcare.org if the breach suggests we need to assist individuals protect against identity theft),
        - who else has been notified (eg. the Privacy Commissioner, Police), and
        - whether any related agencies are likewise affected.

    Refer to the sample notification wording at Appendix B to this Plan, to assist in drafting the above statement.

Privacy notification statements must be approved by the General Manager or Director Corporate Services prior to publication.

If the data breach involves a contracted service provider, funded NGO or other agencies, a **joint notification** should be made on behalf of all organisations, by the organisation with the closest relationship to the affected individuals.

In relation to a data breach involving data received from another agency, the statement **must be sent to the data provider and the NSW Privacy Commissioner** (part of the NSW IPC) **as soon as practicable**. The IPC can be contacted via email to ipcinfo@ipc.nsw.gov.au, or by telephone on 1800 472 679.

The statement **must also be provided directly to affected individuals as soon as practicable**. See further information below about how to do this, under 'How to notify individuals'. NOTE: Where police or another law enforcement agency is investigating the breach, they must be consulted first, before making details of the breach public.

Further matters to consider in relation to notification:

- A proactive media / social media / communications response should also be developed by the Manager Communications.
- Prepare FAQs for internal and external audiences. Depending on the number of individuals affected, we may set up a dedicated webpage, and/or telephone line.

- By publishing Council's stated position early, we demonstrate our transparency and commitment to resolving this matter.
- If there is a risk that the personal information could be used for identity theft or other types of fraud, we may consider engaging with IDCARE, the National Identity & Cyber Support Service.
- There may be others we should contact, such as our insurance company, professional or other regulatory bodies, credit card companies, financial institutions or credit reporting agencies, other internal or external parties, such as third-party contractors, or outsourcing agencies. Also consider groups which represent the affected individuals, such as the relevant union if data about staff was compromised.

7.3.4. Step 4: Prevent future breaches

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. For any High Risk or Medium Risk breaches the Privacy Officer must submit a report within 10 working days to the General Manager outlining the organisational response and mitigation plan.

Mitigation may include: a security audit and any modifications to physical controls such as locks, alarms, visitor access control, review of policies and procedures including the privacy management framework, review of employee training and selection practices, a review of suppliers and third parties, updating passwords, or altered deployments of technology.

8. How to notify individuals

There are three options for notifying individuals at risk of serious harm, depending on what is practicable:

- Directly notify only those individuals at risk of serious harm, or
- Directly notify all individuals whose data was breached, or
- Publicise the statement more broadly.

Where it is possible to identify and contact only those individuals at risk of serious harm, Council must directly notify those individuals. We might also publish the notification more broadly, including on our website.

Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible for us to directly contact all individuals whose data was breached, then Council will directly notify all individuals whose data was breached. We might also publish the notification more broadly, including on our website.

Where it is not possible to identify which individuals might be at risk of serious harm, and it is not practicable to directly contact all individuals whose data was breached (for example, if we don't have up-to-date contact details for old customers), then we must publish a notification on our website. We can also consider other methods of communication such as social media, or advertisements in newspapers.

Where appropriate, social media will be used to provide information about the investigation, any updates and what further action individuals may take and what steps Council is taking to prevent any future data breaches. A media response should also be considered.

Public Notification Register – Council will maintain and publish on our website a public notification register for any public data breach notifications issued. A "public data breach notification" is a notification made to the public at large rather than a direct notification to an identified individual. The MNDB Scheme provides for a public data breach notification to occur in two circumstances:

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

The purpose of the register is to ensure that citizens are able to access sufficient information about eligible data breaches to determine whether they may be affected by the breach and take action to

protect their personal information. The Public Notification Register will contain the following information:

- the date the breach occurred; 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; who to contact for assistance or information; and link to the full public notification.

9. Post-breach review and evaluation

A Data Breach Response Report will be prepared. This report requires the responsible officer (usually the Manager Customer & Compliance or the Manager IM&T) to report on what has been done to prevent a recurrence of the data breach and any changes recommended to our protocols, controls, policies and procedures or staff training etc. Data Breach Response Reports will include:

- A strategy to identify and remediate any processes or weaknesses in data handing that may have contributed to the breach.
- A post-response assessment of how we responded to the breach and the effectiveness of the DBP.

Understanding what went wrong, how issues were addressed and whether changes were needed to processes and procedures following a breach will mitigate future risks and are key to ensuring we continue to proactively manage data breaches in line with regulator and community expectations.

10. 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:

- Maintain and publish (on our website) a public notification register for any notifications given under section 59N(2).
- Establish and maintain 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:

a) who was notified of the breach
b) when the breach was notified
c) the type of breach
d) details of steps taken to mitigate harm done by the breach
e) details of the actions taken to prevent future breaches
f) the estimated cost of the breach.

11. Third party contracts and external service providers

Council is often required to outsource functions to external service providers or another agency (for example, for DA Assessment). These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements. To ensure Council meet its obligations under the PPIP Act, these agreements will be reviewed to ensure they 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.

Appendix A: Data Breach Response Report

1. Contain and assess	
1.1	When did the Data Breach occur (if known)?
1.2	When, how and by whom was the Data Breach first discovered?
1.3	When, how and by whom was the Data Breach first reported to the Privacy Officer?
1.4	What was the primary cause of the Data Breach? • Malicious or criminal attack; System fault; Human error
1.5	Outline the nature of the Data Breach as first reported to the Privacy Officer: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information • Cause of breach / how it occurred • Type of data affected: Financial / Government identifiers (eg. Medicare number or passport number) / Tax File Numbers / Contact information (eg. home address, phone number or email address) / Health information / 'Sensitive information' (e.g. ethnicity, sexuality, religious or political views) / Other • Type of individuals affected • Number of individuals affected
1.6	What steps were immediately taken to contain the Data Breach?
1.7	Who has been drafted into the preliminary Response Team? (Include both internal and external stakeholders. Include the date each role was added.)
1.8	Outline the results of the preliminary fact-finding, about: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information • Cause of breach / how it occurred • Type of data affected: Financial / Government identifiers (eg. Medicare number or passport number) / Tax File Numbers / Contact information (eg. home address, phone number or email address) / Health information / 'Sensitive information' (e.g. ethnicity, sexuality, religious or political views) / Other • Type of individuals affected • Location of individuals affected (eg. whether any are in the EU) • Number of individuals affected

	• Any other entity involved (eg. a contracted third party) • Options to mitigate risk
1.9	What is the preliminary view as to the level of risk posed by the data breach? • High Risk (established) = likely to result in serious harm to affected individual/s • High Risk (suspected/possible, needs further investigation) • Medium Risk • Low Risk
1.10	Have any external parties been notified about the breach? Eg. our insurer; ACORN; other. (Include date and details.)

2. Evaluate and Mitigate	
2.1	Who has now been drafted into the Response Team? (Include both internal and external stakeholders. Include the date each role was added.)
2.2	What steps have been taken to contain the Data Breach?
2.3	What steps have been / should be taken to minimise the effect on potentially affected individuals?
2.4	What steps have been / should be taken to prevent reoccurrence? (Consider here whether any similar breaches have occurred in the past.)
2.5	Concluding the assessment: What is the Response Team's conclusion as to the level of risk posed by the data breach? (Include supporting reasons.) • High Risk = likely to result in serious harm to affected individual/s • Medium Risk • Low Risk

3. Notify and communicate	
3.1	Decision taken in relation to notification? (Include supporting reasons.) • Mandatory (all High Risk breaches) • Voluntary (optional for all other Medium Risk breaches) • No notification (Low Risk breaches)

3.2	Pre-notification steps concluded? (For example, establish telephone hotline, dedicated webpage. Include date completed and details.)
3.3	Statement provided to the Australian Privacy Commissioner (OAIC)? (Include date statement made, how lodged. Attach a copy to this report.)
3.4	Statement provided to the NSW Privacy Commissioner (IPC)? (Include date statement made, how lodged. Attach a copy to this report.)
3.5	What notification method/s have been followed for notifying affected individuals? • Direct to only individual/s at risk of serious harm; Direct to all individuals whose data was breached; Indirect via our website (mandatory if neither of the above is possible); Indirect via other channels eg. social media (an optional extra, in addition to one of the three methods above)
3.6	Notification made to affected individual/s? (Include date notification made, how communicated. Attach a copy to this report.)

4. Review and prevent	
4.1	What has been done to prevent a recurrence of this Data Breach?
4.2	Organisational response and mitigation plan. The following changes are recommended to our: • information security protocols; physical security controls; policies, plans or procedures; staff training; other
4.3	Recommended plan to review / audit to ensure the above corrective actions are implemented

Appendix B: Sample wording of statement

Randwick City Council data breach notification

Dear <NAME-OF-AFFECTED-INDIVIDUAL>

We are contacting you to notify you of an incident of <strike out any of the following if not applicable> unauthorised access to, unauthorised disclosure of, or loss of, personal information held by Randwick City Council.

Security is very important in our operations and the nature of this breach is unusual. Staff at Randwick City Council responded quickly.

On <DATE>, Council became aware that <EXPLANATION-OF-DATA-BREACH (eg. an error which allowed a database containing a certain type of data to be accessed by an unauthorised person, or a file containing X number of records which included the personal information of Y number of customers was accessed / disclosed / lost by our third party contractor Z)>.

We are working with the Office of the NSW/Australian Privacy Commissioner <strike out NSW or Australian as appropriate; the Australian Privacy Commissioner would only be involved if the data breach involved TFNs>, keeping them aware of our efforts to contain the breach and prevent any future similar error from occurring. <INCLUDE IF RELEVANT: The Police have also been informed.>

The personal details <accessed/disclosed/lost> included <WHAT-PERSONAL-INFORMATION (eg. names, addresses, dates of birth etc. and the likely consequences)>.

We want to reassure you that <DETAILS-OF-ANY-ASSURANCE (eg. no passwords, credit card details or bank account details were accessed, disclosed or lost; or no records have been affected or altered in this data breach, so the accuracy of the information we hold about you is unaffected)>.

We are incredibly sorry to our <TYPE OF INDIVIDUALS eg. ratepayers, customers, business contacts>. We are deeply disappointed this could happen. We take full responsibility and are doing everything to not only right this, but to prevent it from happening again.

Randwick City Council is endeavouring to contact all people who are affected by this data breach and inform them of how to further protect their information. We advise you to <WHAT-THEY-SHOULD-DO (eg. change the password you use when dealing with us, and on any other sites where you use the same password; be vigilant reviewing any transactions you have made through our system; review current records / orders; scrutinise emails for suspicious links; cancel credit/debit cards; check your credit history and put a ban on it to prevent any new accounts being opened)> and contact us if you are concerned.

<IF IDENTITY THEFT IS A RISK> To protect yourself from identity theft, you can also contact IDCARE, the National Identity & Cyber Support Service, on 1300 432 273, or via www.idcare.org.

Randwick City Council has taken action to secure the information by <WHAT WE ARE DOING (eg. specify the steps and measures taken to contain the breach, investigate, notify and prevent future data breaches of a similar kind from occurring. This might include employing security experts, carrying out an audit, increasing security and access settings, providing training to staff, or updating policies)>.

<IF THIS IS NECESSARY> We have set up a designated website to keep you informed; see <www.WEB-PAGE-URL>

An officer has also been specifically assigned to answer questions about this data breach and to provide more information, if required.

Contact: <NAME-OF-DESIGNATED-STAFF-MEMBER>

Phone: <XX XX XX>

Email: <xx@xx>

<Keep this paragraph if TFNs were involved, otherwise delete> If you are not satisfied with the actions taken by Randwick City Council, you can lodge a complaint with the Office of the Australian Information Commissioner (OAIC). The OAIC can be contacted in a number of ways:

Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Post: GPO Box 5218; SYDNEY NSW 2001
Website: www.oaic.gov.au

<For all other data breaches, except TFN> If you are not satisfied with the actions taken by Randwick City Council, you can lodge a complaint with the NSW Privacy Commissioner at the Information and Privacy Commission (IPC). The IPC can be contacted at:

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Post: GPO Box 7011, Sydney NSW 2001
Website: www.ipc.nsw.gov.au

FOLLOW US ONLINE

1300 722 542
council@randwick.nsw.gov.au
www.randwick.nsw.gov.au

Randwick City Council
30 Frances Street
Randwick NSW 2031