City of Ryde

Lifestyle and opportunity @ your doorstep

Data Breach Policy

Document Version Control

Document Name:	**Data Breach Policy**
CM Reference:	Record D23/141161: Data Breach Policy
Document Status:	Approved
Version Number:	Version 1.0
Last Review Date:	Wednesday, 10 July 2024
Next Review Date:	01 July 2027
Owner:	City of Ryde | People & Business | Chief Information Officer
Endorsed By:	Executive Leadership Team on 09 July 2024
Distribution:	Internal and External

Change History

Version	Review Date	Author	Reason for Change
0.1	05/10/2023	Enterprise Data and Security Coordinator	Initial draft for review
0.2	08/12/2024	Enterprise Data and Security Coordinator Senior Coordinator IT Infrastructure	Minor updates
0.3	30/01/2024	Chief Information Officer	Clarification re NSW Mandatory Notification of Data Breach (MNDB) scheme as distinct to the Australian Notifiable Data Breaches Scheme.
0.4	26/02/2024	Executive Manager People & Business	Updated draft for internal consultation
0.5	09/05/2024	Chief Information Officer	Revised following consultation feedback including from Privacy Officer.
0.6	30/05/2024	Chief Information Officer	Included reference to NSW OLG Circular 24-06-01.
0.7	07/06/2024	Chief Information Officer	Updated draft addressing feedback from General Manager Business & Operations. Submitted for Executive Leadership Team (ELT) endorsement.
1.0	10/07/2024	Chief Information Officer	Final version addressing feedback from ELT including updated RACI table to ensure CEO, Manager Business Assurance & Governance are INFORMED of reported unconfirmed data breaches.

Contents

1. Purpose

This Policy establishes accountabilities, responsibilities, and process for identifying, assessing, and responding to an eligible data breach originating from Council, or third parties contracted with Council, in compliance with Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) at the City of Ryde Council (**Council**).

2. Scope

This policy applies to all Council employees, Councillors, and any other individuals engaged by Council to perform the role of a public official, including temporary and casual staff, contractors, third-party service providers and suppliers.

3. Policy

Council is committed to managing and responding to a data breach in a timely and effective manner. Effective breach management, including notification where required, assists Council in avoiding or reducing possible harm to affected individuals/organisations and Council.

Part 6A of the PPIP Act establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme. Under the MNDB Scheme, Council has an obligation to:

- immediately make all reasonable efforts to contain a data breach
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach
- notify the Privacy Commissioner and affected individuals of the eligible data breach
- comply with other data management requirements.

4. Definitions

Term	Meaning
CEO	The ***Chief Executive Officer*** or ***head of*** the City of Ryde Council.
Data Breach	Any unauthorised access, disclosure, or loss of data ***held*** by Council.

Eligible Data Breach	s59D(1) of the PPIP Act defines an **eligible data breach** as where: (a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or (b) personal information held by a public sector agency is lost in circumstances where— (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates. (See **5.3 Impact Assessment** for further information on how to test for an eligible data breach.)
Employee	A person who is directly employed by Council on a full time, part time, temporary or casual basis. Also referred to as '*staff*'.
Health Information	A specific type of Personal Information which may include information about a person's physical or mental health or their disability. See Section 6 Definition of "health information" of the Health Records and Information Privacy Act 2002 (HRIP Act).
Held	s59C of the PPIP Act defines personal information is held by a public sector agency if the agency is in possession or control of the information, or the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.
MNDB Scheme	The Mandatory Notification of Data Breach (MNDB) Scheme impacts the responsibilities of agencies under the *Privacy and Personal Information Protection Act 1998* (PPIP Act). It requires

	agencies to notify the Privacy Commissioner and provide notifications to affected individuals in the event of an eligible data breach of their personal or health information by a NSW public sector agency or state-owned corporation subject to the PPIP Act.
Personal Information	Information or an opinion (including information or an opinion forming part of a database and whether or not 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. See Section 4 Definition of "personal information" of the PPIP Act for full definition. Note: For the purposes of the MNDB scheme, Personal Information includes Health Information under s59B of the PPIP Act.
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW) provided for the protection of personal information, and for the protection of the privacy of individuals generally; to provide for the appointment of a Privacy Commissioner; to repeal the *Privacy Committee Act 1975*; and for other purposes.
Public Notification	A notification provided under s59N(2) of the PPIP Act when any or all of the individuals affected by an Eligible Data Breach are unable to be notified individually. Public Notifications are recorded on the Public Notification Register on Council's website.

5. Process for responding to a Data Breach

The following steps outline the process which must be followed by Council employees in relation to any data breach, including a suspected but unconfirmed breach.

5.1. Alert

Where a data breach is known to have occurred (or is suspected) any **employee** who becomes aware of the breach must immediately alert the IT Service Desk **in person,** or **by phone** or **email.**

To contain the breach and minimise the damage the following actions can be authorised by the Chief Information Officer (**CIO**):

- shutting down of applications
- disabling of accounts
- changing of passwords
- restricting access rights
- attempting to locate missing data
- preserve evidence and not tamper with potential crime scene.

5.2. Verification

Once notified of a potential breach the **Enterprise Data and Security Coordinator** must **immediately** consult with the **Senior Coordinator IT Infrastructure** (*or appropriate delegates authorised by the CIO)* to investigate and document key details of the breach, including when it occurred and/or was identified, how it occurred, what data was affected and the extent and impact of the breach. It must also be considered whether the data breach involves **personal information** or **health information**.

Findings are to be reported to the **CIO** by phone and email. The CIO is responsible for notifying the CEO.

5.3. Impact Assessment

Once a breach is confirmed, the **CIO** will determine the key stakeholders and assemble the Incident Response Team (**IRT**) for action as per **Section 6. Roles, accountabilities, and responsibilities**.

The Chief Executive Officer (**CEO**) is responsible for appointing an **assessor** to determine the seriousness of the data breach and if the breach is an **eligible data breach** under the MNDB scheme. That determination is to occur within 30 days[1] of notice of a verified breach.

[1] Note that under Section 59K of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act), where the head of the agency is satisfied that an assessment cannot reasonably be carried out within 30 days, they may approve an extension of time to conduct the assessment. Refer to Guidelines on the assessment of data breaches under Part 6A of the PPIP Act for more information.

Under the **MNDB Scheme** there are two tests to be satisfied to determine an eligible data breach:

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.

Detailed guidance on the assessment of data breaches is contained in the *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act*.

5.4. Rectification

The IRT will determine the rectification required based upon a thorough investigation to determine the root cause of the breach and authorise corrective actions to prevent future breaches.

Lessons learned from the breach will be tracked and documented and used to update relevant policies, procedures, guidelines, and practices.

5.5. Notification

Notifying individuals/organisations affected by a data breach can assist in mitigating damage for those affected individuals/organisations. Notification demonstrates a commitment to open and transparent governance.

In some circumstances it may be appropriate to delay notification, for example where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

If the breach is an **eligible data breach**, and unless an exemption applies, Council will as soon as practicable notify:

1) the NSW Privacy Commissioner via the approved form[2]
2) Individuals/organisations affected by the breach.

[2] See Notify the Privacy Commissioner at https://www.ipc.nsw.gov.au/privacy/mandatory-notification-data-breach-scheme/notify-privacy-commissioner

Council will notify affected individuals or organisations directly by telephone, letter, email or in person.

Public Notification will be provided when any or all of the individuals affected by an eligible data breach are unable to be notified individually, or where direct notification is prohibitively expensive or could cause further harm. The Public Notification will be recorded on the Public Notification Register on Council's website.

The notification will be tailored to the circumstances of the breach. Content of a notification could include:

1) information about the breach, including when it happened
2) a description of what data or personal information has been disclosed
3) assurances (as appropriate) about what data has not been disclosed
4) what Council is doing to control or reduce the harm
5) what steps the person or organisation can take to further protect themselves and what Council will do to assist people with this
6) Council's contact details for questions or requests for information, and
7) the right to lodge a privacy complaint with the Privacy Commissioner.

Depending on the circumstances of the data breach and the categories of data involved, it may be necessary for Council to engage with or notify other external stakeholders in addition to affected individuals and the Privacy Commissioner. These include:

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

The **CEO** will approve all communications with affected individuals and other stakeholders, ensuring transparency and providing guidance on protective measures.

The **Privacy Officer** will provide guidance on privacy and legal obligations.

5.6. Review

Once the data breach rectification and notification has occurred, the IRT will oversee a root cause identification and develop remedial actions that can be taken to reduce the likelihood of recurrence.

This includes a review and remediation of:

- The internal controls in place
- Policies and procedures
- Staff skills and refresher training
- Contractual obligations with contracted service providers.

6. Roles, accountabilities, and responsibilities

The **CEO**, as agency head[3], has specific accountabilities under the **PPIP Act**. Note that only the ***assessor*** responsibility can be delegated by the agency head under the Act.

The **IRT** is responsible for managing and responding to data breaches promptly and effectively. Members of the IRT can include:

1. Chief Executive Officer (CEO)
2. Manager Business Assurance and Governance
3. General Manager Business & Operations
4. General Manager City Shaping
5. Privacy Officer
6. Executive Manager People & Business
7. Chief Information Officer (CIO)
8. Manager Communications & Engagement
9. Risk & Insurance Manager
10. Manager People & Culture.

[3] Agency head accountabilities are defined under the following sections of **Part 6A Mandatory notification of data breaches**:

- s59F Mitigation of harm
- s59G Assessors*
- s59J(2) Decision about data breach
- s59K Extension of assessment period by head of public sector agency
- s59M Public sector agencies must immediately notify eligible data breach
- s59N Public sector agencies must notify certain individuals
- s59P Public notification
- s59Q Further information to be provided to the Privacy Commissioner
- Division 4 Exemptions from certain requirements for an eligible data breach (Sections 59S through 59X)
- s59ZD Public sector agency to publish data breach policy
- s59ZE Eligible data breach incident register
- s59ZJ Delegation by head of public sector agency.

*NOTE: Section 59G(1) states the head of a public sector agency may direct one or more persons to carry out the assessment (each an assessor).

6.1. RACI matrix

Table 1 – Data Breach Policy RACI – confirms the roles & responsibilities of the **IRT** *and other key resources* for each process step in **Responding to a Data Breach**.

ROLES	ACCOUNTABILITIES (RACI) Responsible Accountable Consulted Informed					
	ALERT (Report Breach)	Verification	Impact Assessment	Rectification	Notification	Review
Chief Executive Officer (CEO)	I	C	A	C	A	A
Manager Business Assurance and Governance	I	C	C	C		
General Managers, Business & Operations & City Shaping	I	C	C	C		
Privacy Officer		I	C	C	C	
Executive Manager People & Business	I	I	C	C		
Chief Information Officer (CIO)	I	A	R	A	R	R
Manager Communications & Engagement		I	C	C	C	
Risk & Insurance Manager		I	C	C		
Manager People & Culture		I	C	C		
Senior Coordinator IT Infrastructure	C	C		C		C
Enterprise Data and Security Coordinator	C	R		R		C
Information & Records Manager	I	I		C		
Staff and Councillors	R		I	I	I	C

Table 1 - Data Breach Policy RACI

7. Data breach incident register

Council will maintain an **internal data breach incident register** for compliance and reporting purposes in its records management system according to the requirements of the *State Records Act 1998* and relevant standards. Each eligible data breach will be entered on the register, with the following information included for each entry where practicable:

1. who was notified of the breach
2. when the breach was notified
3. the type of breach
4. details of steps taken by the public sector agency to mitigate harm done by the breach
5. details of the actions taken to prevent future breaches
6. the estimated cost of the breach.

8. Public notification register

Council will maintain and publish on its website a **data breach notification register** for any **public notifications** Council has issued.

9. Training and awareness

All employees and contractors handling personal information will receive training on cyber security data breach prevention, identification, and reporting. This is facilitated through e-learning as part of Council's onboarding processes, as well as part of annual mandatory training.

All Councillors will receive training on cyber security and data breach prevention as part of the onboarding process and on an annual basis throughout the term of Council.

Regular awareness campaigns will be conducted on a quarterly basis to ensure that employees remain vigilant regarding data security.

10. Policy review and revision

This Data Breach Policy will be reviewed a minimum of once every term of Council, or more frequently as required.

All changes to this policy will involve appropriate stakeholder consultation.

11. Document Control

The most current version of this policy will be accessible to all employees through Council's Intranet and Records Management system, and to the public through Council's website.

DATA BREACH POLICY		
Owner: Information & Technology Management (ITM)	Accountability: Chief Information Officer (CIO)	Endorsed: 16/07/2024
CM Reference: D23/141161	Last review date: 10/07/2024	Next review date: 01/07/2027

12. Council guidelines and procedures

Guideline or procedure	Brief description
Privacy Statement	Council's Privacy Statement is published on Council's website and informs the community about how their personal information will be used, stored and accessed after it is collected by the Council.
Privacy Management Plan (D14/8849)	Council's Privacy Management Plan informs the community about how their personal information will be used, stored, and accessed after it is collected by the Council, and informs Council staff of their obligations in relation to handling personal information and when they can and cannot disclose, use or collect it.
Data Breach Incident Register	The Information & Technology Management (ITM) department maintains Council's *internal* register for cyber incidents, including eligible data breaches.
Data Breach Public Notification Register	Published on Council's website the register contains information for any public data breach notifications that Council has 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 register ensures 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.
Acceptable Use of ICT Guidelines for all users	Sets out what users of City of Ryde information and communications technology (ICT) can and can't do, to meet their responsibilities under the ICT Policy and Acceptable Use of ICT Agreement.
IT Disaster Recovery Plan (Ref: D23/139926)	Describes roles, responsibilities, and steps to recover systems and data in case of declared disaster.
Data Breach Response Guideline (Ref: D2019/0091753)	This document outlines responsibilities and processes to identify and address data breach events.

13. Relevant legislation, policies, circulars, and standards

- *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**)
- NSW Mandatory Notification of Data Breach (**MNDB**) scheme
- *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**)
- *Local Government Act 1993* (NSW)
- *State Records Act 1998* (NSW)
- *Crimes Act 1900* (NSW)
- *Crimes Act 1914* (Cth)
- NSW Cyber Security Policy 2023-2024
- 22-39 Release of Cyber Security Guidelines for NSW Local Government (Circular)
- IPC Guide to Preparing a Data Breach Policy May 2023
- IPC Guide to managing data breaches in accordance with the PPIP Act June 2023
- IPC Guidelines on the assessment of data breaches under Part 6A of the PPIP Act September 2023
- NSW OLG Circular 24-06 Privacy and the Mandatory Notification of Data Breach Scheme - Office of Local Government NSW.