Data Breach Response Policy

November 2023

Policy administration

Dates	Policy approved 12/12/2023 This policy is effective upon its approval. Policy review 12/12/2024
Approved by	Executive on 12/12/2023 Executive Team Meeting 12/12/2023
Policy Type	☒ Executive Policy ☐ Council Policy
Exhibition Period	N/A
Policy Owner	Head of Corporate Governance and Risk Business and Corporate Services
Related Documents	Information Security Policy Council's Code of Conduct Privacy Management Plan Business Continuity Management Policy and Plan
Appendices	Appendix A – Data Breach Severity Rating Assessment Appendix B - Data Breach Response Quick Reference Guide
References & Legislation	• NSW Privacy and Personal Information Protection Act 1998 (PPIP Act) • Mandatory Notification Data Breach Scheme within PPIP Act. • Privacy Act 1988 (Office of the Australian Information Commissioner) • Guidelines – Preparing a Data Breach Policy; Regulatory Action under the MNDB Scheme; Assessment of Data Breaches under Part 6A of the PPIP Act; Guide to Managing Data Breaches in Accordance with the PPIP Act ; Exemption for Compromised Cyber Security under Section 59X, Exemption for Risk of Serious Harm to Health or Safety under Section 59W. • Fact Sheets – Notification to the Privacy Commissioner, Exemptions from Notification; Notification to affected individuals • NSW State Records Act 1998
Document Identifier	Policy #: Pol-067.02 Doc #: D23/315767
Breaches of Policy	Breaches of any policy will be dealt with and responded to in accordance with adopted codes and/or relevant legislation.

Record Keeping	All documents and information obtained in relation to the implementation of this policy will be kept in accordance with the NSW State Records Act 1998, Georges River Council's Records and Information Management Policy and adopted internal procedures.

Table of Contents

Purpose

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) establishes the framework for the NSW Mandatory Notification of Data Breach Scheme (MNDB). The MNDB requires Council to notify the Privacy Commissioner and affected individuals of eligible data breaches.

This policy outlines the overall strategy, roles and responsibilities and steps for containing, assessing and managing all data breaches at Council as well as the additional legislative requirements relating to the management of eligible data breaches.

Scope

This policy applies to all staff and Council officials as defined in the Council's Code of Conduct.

Definition of Terms

Term	Meaning
Assessor	Person with delegated authority of the General Manager to undertake data breach assessments in accordance with Section 59G of *the NSW Privacy and Personal Information Protection Act 1998*. Leads the Data Breach Response Team.
Council officials	As defined in Part 2 of Council's Code of Conduct, a Council Official includes councillors, members of staff of Council, contractors, administrators, community members of wholly advisory committees, members of the Audit Risk and Improvement Committee, members of reference panels, council committee members and delegates of Council.
Eligible data breach	An 'eligible data breach' is defined in section 59D of the PPIP Act to mean: 1. there is an 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 2. 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.

Data Breach Response Team	A group of selected roles within Council that is stood up in cases of significant data breaches within Council to manage, investigate and contain the data breach, as well as coordinate the notification to affected parties, and documents Council actions to manage and mitigate the data breach.
Health information	As defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act), ***health information*** means— (a) personal information that is information or an opinion about— (i) the physical or mental health or a disability (at any time) of an individual, or (ii) an individual's express wishes about the future provision of health services to him or her, or (iii) a health service provided, or to be provided, to an individual, or (b) other personal information collected to provide, or in providing, a health service, or (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or (e) healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act. For the purposes of this Policy, personal information includes health information.
Information and Privacy Commission NSW (IPC)	The IPC is an independent statutory authority that administers legislation dealing with privacy and access to government held information in NSW. The Head of Agency is split between two roles – the Information Commissioner and the Privacy Commissioner. Council must immediately notify the Privacy Commissioner of any eligible data breaches.
Mandatory Notification of Data Breach Scheme (MNDB)	The MNDB Scheme requires Council to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

Office of the Australian Information Commissioner (OAIC)	The primary functions of the OAIC are privacy, freedom of information and government information policy. Any eligible data breaches that involve tax file numbers are reportable to the OAIC.
Personal information	Section 4 of the *PPIP Act*, defines ***personal information*** as: information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Serious harm	Harm arising from a data breach that has or may result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Policy Statement

1. What is an eligible data breach?

An eligible data breach (see definitions of terms) can occur between agencies, within an agency, and external to an agency.

The Mandatory Notification Data Breach scheme applies to eligible data breaches of personal information as defined in the definitions section of this policy and *Section 4 of* the PPIP Act, to mean information or an opinion about an individual whose identity is apparent and can reasonably be ascertained from the information or opinion.

Health information as defined in the definitions of terms and Section 6 of the *HRIP Act*, is personal information related to an individual's physical or mental health, disability, and information connected to the provision of a health service. In this Policy personal information includes health information.

For a data breach to become an eligible data breach, this means that the data breach is likely to result in serious harm to individuals whose personal information is involved in the data breach.

If the information subject of an eligible data breach contains tax file numbers and is likely to result in serious harm, it is reportable to both the Australian Information Commissioner of the OAIC under the Commonwealth NDB Scheme and the Privacy Commissioner of the IPC under the MNDB Scheme.

Council must report any form of eligible data breach to the Commissioner using the form provided by the relevant agency (IPC or OAIC) on their website.

2. What is <u>not</u> an eligible data breach?

A data breach is not an eligible data breach if:

- it does not contain personal information, or
- does not contain health information, or
- is not likely to result in serious harm to an individual.

Where a data breach is not assessed to be an eligible data breach, Council is not required to mandatorily notify individuals or the Privacy Commissioner but must still take action to resolve the data breach and may still provide voluntary notification to individuals. In this case Council will not be bound by the rules surrounding the MNDB Scheme.

3. Data breach response

Data breaches must be dealt with on a case-by-case basis by undertaking an assessment of the data breach and risks involved and using that risk assessment to decide the appropriate course of action. Data security methods must be commensurate with the sensitivity of the information and any disciplinary action taken must also be commensurate with the seriousness of the breach.

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

<u>Step 1 Triage and report</u>

i. The person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to immediately contain the breach. For example:

   - Stop the unauthorised practice
   - Recover any records
   - Seek expert assistance – e.g IMT specialist.

ii. The Data Breach Incident Reporting Form (available on Rivernet [Council's intranet] and on Council's web site) must be completed as a priority and submitted online. This form flows to the Data Breach Response Team.

   - An Assessor will be appointed to investigate the data breach. The Assessor will receive the Incident Reporting Form, acknowledge receipt and gather any additional information.
   - The Assessor will identify the Data Custodian.
   - The Data Custodian must complete the Data Custodian Assessment Form. This form is available on Rivernet (Council's intranet).

Step 2: Assess the risk for individuals associated with the breach

i. The Assessor works with the Data Custodian to review the Data Breach Incident Reporting Form and the Data Custodian Assessment Form and will adopt or amend the form as necessary.
ii. The Assessor is responsible for undertaking an assessment and evaluating the risk of serious harm to individuals associated with the breach, as well as the risks to Council, using the Data Breach Impact Severity Ratings Form (Appendix A). The Assessor should escalate medium, high and very high severity risks to the Executive Team immediately. Other risks that have been contained should be put in a report to the Executive Team.
iii. The Assessor may constitute the Data Breach Response Team in one or more of the following circumstances:
    - the risk severity rating is medium or above
    - the data breach is a cyber security incident
    - the data breach relates to information that is determined to be highly confidential or the release may lead to serious harm to Council or a person/s
    - there has been significant community interest in the data breach
iv. The assessment must be completed as soon as practicable, and at the very latest within 30 days to determine whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach.

Step 3: Breach Notification

If an eligible data breach has occurred, Council must:

i. immediately notify the Privacy Commissioner using the approved form.
ii. notify affected individuals as soon as reasonably practicable, unless an exemption applies under Division 4 of the MNDB Scheme. Notification will be direct to each affected person following the Communications Guide within the Data Breach Procedure.
iii. post a notification on its website in the Register of Public Data Breach Notifications, where an affected person is unable to be notified (Section 59N(2) of PPIP).

Optional Notifications

i. The Assessor will consider whether it is appropriate to notify other third parties, such as:
    - The IPC or the OAIC (if tax file numbers are involved).
    - The Police.
    - Insurance providers.
    - Credit card companies, financial institutions.
    - Professional or other regulatory bodies.
    - Other internal or external parties who have not already been notified.

- Agencies that have a direct relationship with the information lost/stolen (example – Health Agencies).

If a data breach is not an eligible data breach under the MNDB Scheme, Council may still consider notifying relevant stakeholders as appropriate and in accordance with the risk rating.

Step 4: Review the incident and take action to prevent future breaches

i. Council will further investigate the circumstances of the data breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence. Depending on the nature of the breach this step may be completed as part of the assessment and mitigation of the breach.

ii. Preventative actions may include:
- a security audit of both physical and technical security controls
- a review of policies and procedures
- a review of employee selection and training practices
- staff training in responding to data breaches effectively.

4. Data Breach Register and Recordkeeping

a) Council will maintain and publish a public notification register for any notifications given under Section 59N(2) of the PPIP Act.

b) Council will also maintain an internal data breach incident register which will include details of the following, where practicable, for all eligible data breaches:
- Who was notified of the breach
- When the breach was notified
- The type of breach
- Details of steps taken by the Council to mitigate harm done by the breach
- Details of the actions taken to prevent future breaches
- The estimated cost of the breach.

5. Processes for responding to incidents that involve another entity

The Data Custodian or contact officer for a third party entity within Council should make contact with the third party as required, or as directed by the Assessor and gather the information required to assess the breach and conduct the risk assessment.

6. Third party contracts and external service providers

Council is often required to outsource functions to external service providers or another agency. These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements, to ensure that Council requires strict data protection requirements of the third parties it interacts with.

Our Statement of Business Ethics outlines the mutual obligations of all third parties who engage with Council, including the requirement to adhere to Council's Privacy Management Plan when handling any private or confidential information, including personal or health information, as well as the requirement to adhere to all Council policies, including the Data Breach Response Policy.

7. Communication Strategy

Any communications issued under this Policy will be developed in consultation with the Coordinator Communications and Engagement and with the approval of the General Manager, and in accordance with Council's Media Policy.

Roles and Responsibilities

Position	Responsibility
General Manager	• Determines if an eligible data breach has occurred in accordance with the PPIP. • Delegates an assessor to lead the investigation under Section 59G of the PPIP. • Has the ability to approve an extension of the assessment period as per Section 59K of the PPIP. • Notifies the Privacy Commissioner of an eligible data breach. • Has the ability to approve an exemption under Division 4 of the PPIP.
Assessor	• Delegated by the General Manager to conduct Assessments in accordance with Part 6A of the PPIP Act. • Carries out the assessment of the data breach. • Nominates a Data Custodian. • Constitutes a Data Breach Response Team in one or more of the following circumstances and in accordance with this policy: - If the risk severity rating is medium or above - If the data breach is a cyber security incident - Data that is highly confidential or the release may lead to serious harm - Significant community interest. • Consult with internal and external stakeholders as required. • May seek guidance from experts as required. • Provides a recommendation to the General Manager as to whether it is an eligible data breach. • Notification to affected parties, Police, Privacy Commissioner as applicable. • Reports actions to the Director / General Manager. • Prepare a data breach review report for each separate data breach incident, for submission to the Executive Team. • Follow this policy when responding to a data breach. N.B: A person who is reasonably suspected as being involved in an action or omission that led to the breach is not permitted to be an assessor.

Data Breach Response Team	• Assemble promptly to review and respond to a data breach, when constituted by the Assessor. • The Data Breach Response Team will consist of people selected by the Assessor, depending on the type of data breach that has occurred. The Response Team may consist of: - The Assessor - The Data Custodian - Chief Information Officer - Head of Technology - Head of Information Management - Team Leader Records and Information Management - Team Leader Technology Systems and Integration - General Counsel - Senior Solicitor - Manager City Life - Coordinator Communications & Engagement - Manager Corporate Governance and Risk Management - Manager Office of the General Manager - Director Business and Corporate Services - General Manager - Head of Business Insights - Enterprise Systems Specialist
Data Custodian	• Identified by the Assessor. • Usually the Manager of the area where the data breach has occurred. • Conducts preliminary risk assessment and completes Data Custodian Assessment Form (available on Rivernet). • Undertakes remedial actions as required by the Assessor.
Director of Business and Corporate Services	• Alternate Assessor. • Receives initial Data Breach Incident Reporting Form.
Head of Corporate Governance and Risk	• Primary Assessor. • Receives initial Data Breach Incident Reporting Form. • Conduct awareness of this policy within Council periodically. • Publication of Public Notifications Data Breach Register on Council's website. • Maintains internal eligible data breach register. • Notification to Insurers of an eligible data breach that is reported to the Privacy Commissioner. • Notification to Privacy Commission of the IPC and Australian Information Commissioner of the OAIC if tax file numbers are involved in a data breach.
Chief Information Officer	• Receives initial Data Breach Incident Reporting Form. • Co-ordinates remedial actions as required by the Assessor or in the event of a cyber security incident.
Head of Technology	• Maintenance of systems following recommendations from CyberSecurity NSW and best practice. • Cyber Security awareness training of all staff. • Assessment of impact for electronic data breach.

	• Coordinates technical staff during the assessment and within the Data Breach Response Team. • Reports and documents actions for the Chief Information Officer and Assessor.
Chief People Officer	• Coordinates support services for staff who have personal information breached by the Council.
Head of Information Management	• Coordinates Records and Information Management staff during the assessment and within the Data Breach Response Team. • Maintenance of forms. • Backup for IMT coordination.
General Counsel	• Alternate Assessor. • Receives initial Data Breach Incident Reporting Form.
Coordinator Communications and Engagement	• Coordinate release of information on Council's website and media or press release as deemed appropriate by the General Manager, and in accordance with the Communication Strategy included in this Policy.
Contract-owners within Council	• Inclusion in Contacts for third parties such as contractors with regard to their data breach responsibilities, how they should respond and contact should they have a data breach.
All Staff	• Ensure that they have read this policy. • Comply with the PPIP and HRIP Acts including protecting personal information held by the Council from unauthorised access, disclosure or loss. • Maintain electronic devices in accordance with the directions of the CIO. • Report suspected data breach including facts, documents and screen prints where possible. • Promptly respond to requests for information from the Assessor.

Version Control and Change History

Version	Amendment Details	Policy Owner	Period Active
1.0	Complete new Georges River Council Data Response Framework Policy Policy approved by ET 18/09/18, with minor amendments following feedback from ARIC at	Chief Information Officer	15/02/2019 – 12/12/2023

	their meeting on 15/02/19.		
2.0	Implementation of the MNDB Scheme within the PPIP Act 1998. Policy updated.	Head of Corporate Governance and Risk	12/12/2023 – 12/12/2024

Appendix A – Data Breach Impact Severity Rating Assessment

DATA BREACH IMPACT SEVERITY RATINGS FORM					
Impact Type	**Severity** **Lowest ←----------→ Highest**				
Impact Severity	**1. NEGLIGIBLE**	**2. LOW**	**3. MEDIUM**	**4. HIGH**	**5. VERY HIGH**
Risk to individual safety due to unauthorised access or disclosure of classified information	No injury/minimal risk to personal safety	Single injury/low risk to personal safety of client/employee	Multiple injuries/moderate risk to safety of client/employee	Death/disabling injury/high risk to safety of client/employee	Multiple deaths or disabling injuries/very high risk to safety of client/employee
Distress caused to any party or damage to any party's standing or reputation	Negligible, no public concern – only routine internal reporting	Minor distress, minor damage – visible limited/localised media interest, internal reporting	Substantial short term distress – restricted negative publicity from local media, internal inquiry	Substantial long term distress – main stream media report, internal inquiry	Substantial long term distress to multiple parties – broad public concern and media coverage.
Non-compliance – unauthorised release of information classified as Personal to a third party	Minor compliance issues – no or negligible impact, offence punishable by warning / no fine	Short to medium term action required – minor impact, offense punishable by small fine	Immediate action needed to achieve compliance – measurable impact, offense punishable by minor fine	Shutdown of service for non-compliance – significant impact, offence punishable by major fine.	Shutdown of multiple services for non-compliance – major consequences to a person or council
Threat to Council's capacity to deliver services due to Information Security breach	No or negligible threat to, or disruption of business or systems or service delivery	Minimal threat to, or disruption of localised business or systems or service delivery	Moderate threat to or cessation of a service for a week, and subsequent disruption	Multiple essential/critical services impaired, or disrupted over a month	Cessation of multiple essential/critical services for several months
Impact on Council finances, economic or commercial interests	No or negligible impact – consequences resolved by routine operations	Minor impact on finances, economic or commercial interests	Moderate impact – disadvantage caused to the government in commercial or policy negotiations	Substantial – damage to finances, economic or commercial interests	Substantial – damage to finances, economic or commercial interests
Impact on development or operation of major government policy	No or negligible impact – consequences resolved by routine operations	Minor – impact on efficiency or effectiveness, managed internally	Impede effective development or operation – significant review or changes required	Seriously impede development or operation – project or program may not survive	Substantially impede operation or development
Action required	Data Breach Incident Reporting Form to be submitted and actions taken as directed by the Assessor	Data Breach Incident Reporting Form to be submitted and actions taken as directed by the Assessor	Report to be submitted to Data Breach Response Team, and if appropriate Director / General Manager & Privacy Commissioner if an eligible data breach. Data Breach Response Team to be activated.	Report to be submitted to Data Breach Response Team, Director, General Manager and Privacy Commissioner if an eligible data breach. Data Breach Response Team to be activated.	Report to be submitted to Data Breach Response Team, Director, General Manager & Privacy Commissioner if an eligible data breach. Data Breach Response Team to be activated.

NB: This table is to be used for assessing the data breach. To ascertain whether the data breach is an eligible data breach, see Section 1 of this policy. Eligible data breaches have additional requirements as set out in the PPIP and this policy.

Appendix B – Data Breach Response Quick Reference Guide