1. Purpose

Council is committed to protecting the personal information it holds and ensuring compliance with the *Information Privacy Act 2009* (Qld) (IP Act) and the Mandatory Notification of Data Breach (MNDB) scheme. This Data Breach Policy outlines the steps Council will take to respond to a data breach, including suspected or confirmed eligible data breaches.

This policy ensures that Council responds to data breaches in a timely, coordinated and transparent manner, including assessing suspected breaches, containing and mitigating harm, notifying affected individuals where required, and meeting all reporting obligations under the Mandatory Notification of Data Breach scheme. It also establishes clear roles and responsibilities to support consistent and effective breach management across Council.

2. Scope

This policy applies to all Councillors, volunteers, employees and contractors working for Council regardless of whether they are permanent, temporary, full-time, part-time or casual.

This policy applies to all personal information that is collected, stored, used or disclosed by Council in all aspects of its operations and performance.

This policy applies to all Council information systems, digital platforms, mobile devices, paper records, cloud-based services and third-party applications where personal information is created, received, stored, processed or transmitted. It also applies to personal information handled during Council-related activities conducted off-site or outside normal business hours.

3. Responsibility and Roles

Each employee and elected member of Council are required to manage corporate information in the course of their duty or under their direct control and that are subject to legislation relating to *Public Records Act 2023* and the IP Act.

ROLE	RESPONSIBILITY
Elected Members, Employees, Contractors and Volunteers	• Read the Data Breach Policy and Response Plan and understand what is expected of them. • Comply with the IP Act, including protecting personal information held by the agency from unauthorised access, disclosure or loss. • Immediately report any data breach or suspected data breach to your supervisor, manager, senior officer, the designated Privacy Officer (PO) and/or a member of the Data Breach Response Team (DBRT). • Respond to requests for information from and cooperate with the Privacy Officer and/or the DRBT. • Comply with record keeping obligations.
Privacy Officer	• Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.

	• Escalate serious data breaches to the Business Services Coordinator, the Director Corporate, Community and Development Services (DCCDS) or relevant senior officers. • Notify, or arrange for a senior officer, to notify the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to the agency website under section 53(1)(c). • Immediately report a data breach that is also a cyber security incident to the Information Services Manager, if not already reported. • Maintain the Register of Eligible Data Breaches.
Senior Leadership Team Member	• Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy. • Immediately report a data breach that is also a cyber security incident to the Information Services Manager, if not already reported.
Executive Leadership Team Member	• Immediately report a cyber security incident that is also a data breach to the Privacy Officer, if not already reported. • Where relevant, notify the Information Commissioner, affected persons and others where required. • Implement the Cybersecurity Management Plan and related procedures if the data breach is also a cyber security incident. • Convene the Data Breach Response Team, when appropriate.
Data Breach Response Team (DBRT)	• Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems.
Business Services Coordinator	• Maintain and update this Policy.

4. Definitions

Affected Person means an affected individual under section 47(1)(ii) and (b)(ii) of the IP Act.

Data Breach - Data Breach, of an agency, means either of the following in relation to information held by the agency:

(a) unauthorised access to, or unauthorised disclosure of, information; or

(b) the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

Refer to Schedule 5 of the IP Act.

Data Breach Response Plan is a document that outlines how Council responds to actual or suspected data breaches to manage risk, meet legal obligations, and protect personal information.

Data Breach Response Team is made up of:

- Governance Support Officer;

- Senior Records Officer;
- Business Services Coordinator;
- Information Services Manager;
- Director Corporate, Community and Development Services; and
- Chief Executive Officer.

Eligible (Notifiable) Data Breach is data breach that is reasonably believed to be likely to result in serious harm to an individual to whom the information relates, and which triggers notification obligations under Part 3A of the IP Act.

Information Commissioner means the Queensland Information Commissioner.

IP Act means Information Privacy Act 2009 (QLD)

Personal information in accordance with s12 of the IP Act, personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:

(a) whether the information or opinion is true or not, and

(b) whether the information or opinion is recorded in a material form or not.

Serious Harm includes serious physical, psychological, emotional, economic or financial harm, or serious harm to an individual's reputation, arising from the unauthorised access to, or disclosure of, their personal information.

Privacy Officer means the Senior Records Officer, or an Officer delegated by the Chief Executive Officer.

Sensitive Personal Information is a subset of personal information that is given a higher level of protection due to its nature, including health information, financial details, identity documents, or other information that could result in significant harm if misused.

Agency as defined under the Information Privacy Act 2009 (Qld), includes a department, local government or other public sector unit that is subject to the Act. For the purposes of this policy, this refers to Council.

Cyber Security Incident an event or activity that compromises, or has the potential to compromise, the confidentiality, integrity or availability of Council's information systems, including unauthorised access, malware attacks, ransomware, or system intrusion.

Containment are actions taken to limit or stop the impact of a data breach, including recovering information, shutting down systems, revoking access, or preventing further unauthorised disclosure.
Remediation means actions taken to address the causes and consequences of a data breach and to prevent recurrence, including system improvements, policy updates and staff training.

Eligible Data Breach Register is a formal internal record maintained by Council documenting all eligible data breaches in accordance with section 72 of the IP Act.

5. Policy

5.1 Managing Data Breaches

A data breach may be accidental or deliberate and includes any unauthorised access to, disclosure of, or loss of personal information. Council will manage all suspected and confirmed data breaches promptly to minimise harm to individuals, protect Council systems and meet its obligations under the Mandatory Notification of Data Breach scheme.

Council will respond to data breaches in accordance with the Data Breach Response Plan, based on the following principles:

Stage 1: Preparation

Council will take proactive steps to ensure it is prepared to effectively manage a data breach. Preparation activities include:

- Providing regular training to employees, Councillors and contractors on privacy obligations, data breach identification and reporting requirements;
- Ensuring policies, procedures and frameworks are maintained and aligned with the IP Act;
- Key roles and responsibilities are defined and understood by those who hold specific positions;
- Incident Reporting mechanisms are implemented and are accessible to all employees;
- Undertake Privacy Impact Assessments (PIA's) where appropriate and managing risks in accordance with Council's Risk Management framework; and
- Periodically reviewing and testing data breach response processes to ensure effectiveness.

Stage 2: Identification and Internal Reporting

All staff must **immediately** report suspected or actual data breaches to the Privacy Officer and/or their supervisor.

Once a suspected breach is reported, the Privacy Officer will record the incident in the Data Breach Register, conduct an initial assessment to determine the severity and scope of the breach, and coordinate with relevant staff to activate the Data Breach Response Plan. Where necessary, Information Services, Records Management or external specialists may be engaged to support the assessment.

Stage 3: Containment and Mitigation

Depending on the nature of the data breach, the relevant staff member will take all reasonable steps to contain or prevent further damage from the breach. Subsequently, the DBRP will take all necessary steps to contain the breach, inclusive of seeking external assistance when required. The objective being to lessen the likelihood of harm and to act as soon as practicable.

Stage 4: Assess the Risk

Council will assess whether the reported breach is an Eligible Data Breach, considering the kinds of personal information involved, the sensitivity of the information, the likelihood that any protective measures will be overcome, and the nature and seriousness of any harm to affected individuals likely to result from the data breach.

Stage 5: Notification

Individuals affected by the Eligible Data Breach
As soon as practicable after forming a reasonable belief that a data breach is an ***Eligible Data Breach***, Council will take the steps set to notify individuals and provide them with the information required in section 53(2) of the IP Act.

The Information Commissioner
Unless an exemption applies, agencies must notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an ***Eligible Data Breach***. Agencies may seek advice from the Office of the Information Commissioner about a data breach, but notification of an Eligible Data Breach must be made in writing.

Stage 6: Review and Remediation

Council will perform a post-incident review, including:

- update systems, processes and the response plan as necessary;
- identify lessons learned and implement improvements to prevent future breaches; and
- implement recommendations from the review and ensure they are documented in the Eligible Data Breach Register.

Council is committed to continuous improvement in information security and privacy management. Insights gained from data breach reviews will be used to strengthen policies, systems, training and risk controls to reduce the likelihood and impact of future breaches.

6. Register of Eligible Data Breaches

Under section 72 of the IP Act, agencies must keep an internal Register of Eligible Data Breaches. This Register will be updated as part of the Data Breach Response Plan.

The Register will record details of all Eligible Data Breaches, including the date of the breach, a description of the incident, the types of personal information involved, actions taken to contain and assess the breach, notifications made, and any remediation or improvements implemented. The Privacy Officer is responsible for maintaining the Register and ensuring entries are accurate, complete and retained in accordance with the *Public Records Act 2023*.

7. Record keeping

All records relating to an Eligible Data Breach must be retained in accordance with the *Public Records Act 2023* and Council's Records Management Policy. This includes assessment documents, notifications, containment actions, review outcomes, and entries in the Eligible Data Breach Register. The Privacy Officer is responsible for ensuring that all relevant documentation is complete, accurate and captured in the Electronic Document and Records Management System (EDRMS) as part of the official record of the incident.

8. Related Legislation

- *Information Privacy Act 2009 (Qld)*
- *Information Privacy and Other Legislation Amendment Act 2023 (Qld)*
- *Information Privacy Regulation 2025 (Qld)*
- *Mandatory Notification of Data Breach Scheme (Chapter 3A, IP Act)*
- *Public Records Act 2023 (Qld)*
- *Local Government Act 2009 (Qld)*
- *Right to Information Act 2009 (Qld)*

9. Associated Documents

- Privacy Policy;
- Data Breach Response Plan;
- Data Breach Register;
- Data Breach Details Form;
- Data Breach Notification Letter Template; and
- Records Framework.
- Code of Conduct
- Councillor Code of Conduct

DOCUMENT HISTORY AND STATUS			
Policy Number	919	**Version**	1
Approved By	Council Resolution # 3062026-13	**Approval Date**	30 June 2026
Initial Date of Adoption	30 June 2026	**Next Review Date**	June 2028
ECM Number	2798818	**Document Contact**	Business Services Coordinator