	Data Breach Policy	**POLICY NO.** COR 1056

1. Background and Context

Cloncurry Shire Council is dedicated to protecting the integrity and confidentiality of the personal information entrusted to us by our community, ensuring it remains secure against loss, misuse, or unauthorised access and disclosure. This policy defines Council's operational framework for identifying, evaluating, and responding to data breaches. By implementing these practices, Council ensures full compliance with the mandatory data breach notification requirements established under Chapter 3A of the *Information Privacy Act 2009* (Qld).

2. Scope

This Policy is mandatory and applies to all personnel who access, handle, or manage information repositories held by Cloncurry Shire Council. This includes:

- All Council employees (full-time, part-time, and casual) and Councillors;
- Independent consultants, volunteers, and work-experience students; and
- External third-party suppliers, software vendors, and contractors.

2. Objectives

The purpose of the Policy is to:

- Establish a transparent, legally compliant operational framework for identifying, managing, and resolving data breaches within Council.
- Protect the fundamental privacy rights of individuals and safeguard the security of all personal information held in Council custody.
- Ensure Council meets its strict statutory requirements to complete initial triage and formal assessments within the legally mandated 30-day window.
- Minimise the potential for serious physical, psychological, emotional, financial, or reputational harm to individuals affected by data exposure.
- Provide a structural methodology to learn from information security incidents and continuously strengthen Council's data protection measures.

3. Definitions

Role	Definition
Agency Worker / Employee	A person who carries out work in any capacity for an agency as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including employees, contractors, subcontractors, apprentices, trainees, work experience students, or volunteers.
Affected Individual	An individual whose personal information was involved in a data breach, and who faces a likelihood of experiencing serious harm as a result of that occurrence.
Contracted Service Provider / Contractor	Any external individual, consultant, vendor, or commercial partner engaged by Council to execute tasks or provide

	software platforms that handle personal information held by Council.
Data Breach	The unauthorised access to, unauthorised disclosure of, or loss of information held by an agency where unauthorised access or disclosure is likely to occur.
Eligible Data Breach	A data breach involving personal information held by an agency where the unauthorised access, disclosure, or loss is objectively assessed as being likely to result in serious harm to any of the individuals to whom the information relates.
Held / Hold	Personal information is held by Council if it is contained in a document in the physical possession or under the digital control and statutory custody of Council, including within cloud environments managed by third parties.
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether true or not, and whether recorded in a material form or not.
Sensitive Information	A specific category of personal information carrying heightened security risks, including data regarding an individual's racial/ethnic origin, political opinions, religious beliefs, philosophical alignments, trade union memberships, sexual practices, criminal records, health details, or biometric templates.
Serious Harm	Substantial detrimental effects on an individual which extend beyond minor annoyance or irritation, including severe physical danger, psychological trauma, emotional distress, financial loss, or significant harm to the individual's reputation.

4. Roles and Responsibilities

Role	Definition
All Employees & Agency Workers	A person who carries out work in any capacity for an agency as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including employees, contractors, subcontractors, apprentices, trainees, work experience students, or volunteers.
IT Coordinator	Act as the primary centralised portal for intake of all data breach notifications transmitted to council@cloncurry.qld.gov.au. Initiate immediate technical containment protocols to halt ongoing data exposure, isolate systems, or revoke compromised credentials. Conduct initial technical assessments to log the scope of system activity, identify affected data sets, and determine if an information security incident involves personal information. Cross-

	escalate all technical findings swiftly to the Risk & Governance Coordinator for formal statutory tracking.
Governance & Risk Coordinator *(Acting Privacy Officer)*	Receive technical triage inputs and lead the formal evaluation of the severity and likelihood of serious harm to individuals. Drive the data breach assessment process forward to ensure compliance with the strict 30-day statutory window. Escalate serious data breaches to senior management and executive leaders. Coordinate and draft the required statutory notification paperwork for the Information Commissioner and affected individuals. Manage, monitor, and publish public notices on Council's website when direct communication is unfeasible. Maintain and update this Policy annually and secure the internal Register of Eligible Data Breaches.
Contractors, Subcontractors & Third-Party Suppliers	Adhere strictly to this Policy and enforce robust security frameworks over all Council data within their operational control. Issue a direct report detailing all material facts of any actual or suspected data breach to the IT Coordinator via council@cloncurry.qld.gov.au immediately, and no later than 24 hours after detection. Provide extensive technical cooperation, logs, and system data to Council during the statutory evaluation window.
Managers and Supervisors	Identify and escalate information handling vulnerabilities within their respective operational units. Ensure any data breach flagged by their staff is immediately directed to the IT Coordinator for processing.
Senior Management & Chief Executive Officer	Assume ultimate accountability for ensuring information assets under Council control align with the *IP Act*. Formally authorise and execute all outward-facing notification statements sent to the Information Commissioner and the public. Convene the Data Breach Response Team when an incident threatens systemic risks or widespread community harm.
Data Breach Response Team	An ad-hoc leadership group convened by Executive Management to steer the containment, mitigation, and remediation of data breaches likely to cause critical harm to individuals or Council infrastructure.

6. Policy

Cloncurry Shire Council manages all actual or suspected data breach events through an integrated 6-stage operational cycle. This methodology ensures that vulnerabilities are contained immediately while satisfying all statutory evaluation criteria:

- **Stage 1: Preparation** – Council implements a defensive architecture of data security rules, network access controls, user credential auditing, and mandatory information privacy awareness programs to block threats and eliminate handling errors.
- **Stage 2: Identification** – Potential data breaches are detected via automated system monitors, employee feedback, or public reports. Any worker or contractor who suspects a data breach must bypass internal hierarchies and report it directly to council@cloncurry.qld.gov.au.
- **Stage 3: Containment and Mitigation** – Upon receipt of a report, the IT Coordinator immediately executes reasonable mitigation manoeuvres. This includes isolating compromised servers, recalling misdirected emails, terminating active system access codes, or recovering physical data assets from unauthorised recipients.
- **Stage 4: Assessment** – The Governance & Risk Coordinator steps in to execute an objective assessment regarding whether the event constitutes an Eligible Data Breach. This analysis evaluates the sensitivity of the data, the security protections in place (such as encryption), the types of unauthorised persons who gained access, and whether the harm is probable rather than merely possible. Council must take all reasonable steps to finalise this assessment within 30 days.
- **Stage 5: Notification** – If an Eligible Data Breach is validated, Council will expeditiously provide a formal statement to the Queensland Information Commissioner. Impacted citizens will be notified directly with clear descriptions of the breach, the exact data categories involved, and actionable recommendations on how they can protect themselves. If individual contact details are missing, Council will prominently display a Public Notification notice on its website for a minimum of 12 months.
- **Stage 6: Post-Data-Breach Review and Remediation Evaluation** – Following resolution, Council will review the root causes of the vulnerability, evaluate control failures, update internal documentation, and deliver targeted training to prevent similar security incidents.

7. Accountability and Reporting

- Pursuant to Section 72 of the *Information Privacy Act 2009* (Qld), Council maintains a centralised, private internal Register of Eligible Data Breaches. The Governance & Risk Coordinator holds direct accountability for updating this register, which must detail the chronological timeline, nature, scope, mitigation actions, and statutory notification choices for every confirmed incident.
- Council mandates the thorough documentation of every reported data vulnerability, including incidents that do not cross the legal threshold into an Eligible Data Breach. All initial assessment forms, digital telemetry logs, executive briefs, and notification records will be securely archived within Council's Electronic Document and Records Management System (EDRMS) in complete compliance with the *Public Records Act 2023* (Qld).

8. References and Related Documents:

- *Information Privacy Act 2009* (Qld)
- *Public Records Act 2023* (Qld)
- *Work Health and Safety Act 2011* (Qld)
- Information Privacy Policy - COR 1047

POLICY VERSION AND REVISION INFORMATION

Version No.	Approval	Date Approved	Review Date
1.0	Council Resolution 110.2026	16 June 2026	June 2028

Policy Approved by: Tammy Parry

Title: Chief Executive Officer