G.124 DATA BREACH POLICY

1 OBJECTIVE

Quilpie Shire Council is committed to safeguarding the personal information it holds and ensuring compliance with the *Information Privacy Act 2009 (Qld)* and *Information Privacy and Other Legislation Amendment Act 2023 (IPOLA).* This Data Breach Policy outlines the steps Council will take in responding to a data breach, including any suspected or confirmed eligible data breaches.

2 SCOPE

This policy applies to all Quilpie Shire Council Councillors, employees, contractors, and volunteers who handle personal information.

3 STATEMENT

3.1 OVERVIEW

A data breach can occur in many ways — through malicious third-party activity, internal human error, or failures in information handling or security systems. However, not every data breach will meet the threshold of an Eligible Data Breach. Only breaches that satisfy the criteria for an Eligible Data Breach will trigger the Mandatory Notification of Data Breach (MNDB) requirements.

An eligible data breach occurs when there is unauthorised access to, or disclosure of, personal information, or loss of information in circumstances where unauthorised access or disclosure is likely, and the breach is likely to result in serious harm**.**

Council will respond to any data breach promptly and effectively to minimise harm, meet legal obligations, and strengthen its systems and processes. Council will maintain a Data Breach Response Plan and maintain a register of eligible data breaches and ensure all staff understand their responsibilities under this policy.

3.2 KEY ROLES AND RESPONSIBILITIES

- All Staff
  - Read the Data Breach Policy and Data Response Plan and understand what is expected of them.
  - Comply with the *Information Privacy Act (Qld) 2009* and *Information Privacy and Other Legislation Amendment Act 2023 (IPOLA)*
  - Required to report suspected breaches immediately.
  - Respond to requests for information from and cooperate with the Data Breach Response Team.
  - Comply with record keeping obligations.
- ICT Officer
  - Assists with technical containment and investigation of all breaches.
- Director and Deputy Director Corporate Services
  - Coordinates breach assessment, containment, and notification.

- 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) of the *Information Privacy Act (Qld) 2009*.
- Maintains the Register of Eligible Data Breaches
- Maintains and updates this policy.

- Chief Executive Officer (CEO)
  - Oversee all breach responses and approve notifications.

3.3 DATA BREACH RESPONSE PROCESS

Council has developed a Data Breach Response Plan that outlines its response process. This plan is reviewed on a regular basis to ensure relevancy and efficiency.

3.1.1 Identification

All suspected and eligible data breaches are reported as a matter of priority to the Director/ Deputy Director of Corporate Services.

3.1.2 Containment

Depending on the nature of the data breach the relevant officers will work to contain the incident by restricting access, recovering records, and reinforcing system security.

3.1.3 Assessment

Assess the types of personal information involved in the data breach including the extent, sensitivity and the nature and seriousness of any harm to any affected individuals involved.

3.1.4 Notification

If the data breach is deemed to be eligible, notification is required to the Information Commissioner, affected individuals and other agencies or organisations, including any relevant exemptions.

3.1.5 Review and Remediation

Review the data breach incident, which includes:

- Recording the incident in Council's Data Breach Register
- Review effectiveness and response
- Update systems, processes and procedures as necessary
- If necessary, provide training for staff

3.4 RECORDKEEPING

In accordance with section 72 of the *IP Act,* Council will maintain a register of eligible data breaches. This register and all records related to data breaches will be managed in compliance with the *Public Records Act 2023*.

3.5 TRAINING

Council will provide all staff with training on data breach identification. Updates and changes to legislation will be provided to all necessary staff as well as updates to the Data Breach Policy and this procedure.

3.6 PRIVACY COMPLAINTS

If a member of the public is not satisfied with the manner in which Council has dealt with their personal information or handled their request for access / amendment to their personal information under the *Information Privacy Act 2009*, they may lodge a privacy complaint. The privacy complaints process can be found under Council's Personal Information Privacy Policy on Council's website.

4 HUMAN RIGHTS COMPATIBILITY STATEMENT

This Policy has been assessed as compatible with the Human Rights protected under the *Human Rights Act 2019.*

5 DEFINITIONS

Data Breach	When personal information is lost, accessed or disclosed without authorisation
Eligible Data Breach	A data breach likely to cause serious harm and requires mandatory notification
Personal Information	Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, 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

6 RELATED POLICIES | LEGISLATOIN | OTHER DOCUMENTS

- *Information Privacy and other Legislation Amendment Act 2023*
- *Information Privacy Act 2009*
- *Public Records Act 2023*
- *Privacy Act 1988 (Cth)*
- *Right to Information Act 2023*
- *Australian Privacy Principles*

IX #	Details

274177	G.124 Data Breach Response Plan
274387	G.12 Personal information privacy policy

7 VERSION CONTROL

V1	24-Feb-24	Developed and distributed