# Data Breach Policy

| | | | |
|---|---|---|---|
| Policy Type | Governance Policy | Version: | 1.0 |
| Responsible Officer | Manager Information Systems & Governance | Date Approved: | 20/08/2025 |
| Review Officer: | Director Corporate & Community Services | Review Due: | 20/07/2029 |
| Author: | Manager Information Systems & Governance | Commencement: | 20/08/2025 |

## 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.

## 2. SCOPE

This Policy applies across Council.

## 3. POLICY STATEMENT

### 3.1 OVERVIEW

Council will respond promptly and effectively to any data breach to minimise harm, comply with legal obligations, and improve its systems and processes. We will maintain a register of eligible data breaches and ensure all staff are aware of their responsibilities under this policy.

### 3.2 KEY ROLES AND RESPONSIBILITIES

#### 3.2.1 *Manager Information Systems & Governance*

Coordinates the data breach response, conducts risk assessments, and convenes the Data Breach Response Team.

#### 3.2.2 *Senior Advisor Governance & Compliance*

Receives data breach reports and performs initial assessment.

#### 3.2.3 *Data Breach Response Team (response team)*

A multidisciplinary team convened to manage significant data breaches. Members may include representatives from Senior Management, Governance & Compliance, Human Resources and Communications teams.

#### 3.2.4 *All Staff*

Required to report suspected breaches immediately and perform initial containment actions.

### 3.3 DATA BREACH RESPONSE PROCESS

Council has developed a *Data Breach Response Plan* (response plan) that details its response process. It is reviewed and tested on a regular basis to ensure relevancy and efficacy. The response plan encompasses five major steps:

#### 3.3.1 *Identify the breach*

All real or suspected data breaches are escalated by staff as a matter of priority.

#### 3.3.2 *Contain the breach*

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 response team has a mandate to 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 practical.

#### 3.3.3 *Assess the Risk*

Evaluate 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.

#### 3.3.4 *Consider Notification*

If the breach is assessed as eligible, make notifications to the Information Commissioner and affected individuals, including any relevant exemptions. This may also involve contacting other agencies or affected organisations.

#### 3.3.5 *Review Incident*

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
- implement recommendations from the review and ensure they are documented in the Eligible Data Breach Register

### 3.4 RECORDKEEPING

Council will maintain a register of eligible data breaches in accordance with section 72 of the IP Act. This register will include details of each breach, the response, and any notifications made. All records will be managed in compliance with the *Public Records Act 2023* (Qld).

### 3.5 TRAINING AND AWARENESS

Council will provide regular training to staff on their responsibilities in relation to privacy and data breaches. This will include guidance on identifying and reporting breaches and understanding the MNDB scheme.

### 3.6 PRIVACY COMPLAINTS

If you become aware of a data breach involving personal information that we hold about you, and if you believe that we have failed to handle your personal information appropriately, you can make a privacy complaint.

Council's *QPP Privacy Policy*, which is available on our website, provides information on how to make a privacy complaint to us.

## 4. REPORTING

Currently there is no MNDB scheme specific to Queensland Local Government agencies however, such a scheme will be effective from 1 July 2026. As per Office of the Information Commissioner recommendation, Council has adopted a voluntary stance and will operate as if a mandatory scheme is in effect.

## 5. DEFINITIONS

**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, the information;

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

**Eligible data breach** is a data breach that is likely to result in serious harm to any individual whose personal information is involved, as defined under 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**, to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

(a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or
(b) serious harm to the individual's reputation because of the access or disclosure.

## 6. RELATED DOCUMENTS AND REFERENCES

*Data Breach Response Plan* (MSC)
*Information Privacy Act 2009* (Qld)
*Public Records Act 2023* (Qld)
*QPP Privacy Policy* (MSC)

## 7. REVIEW

It is the responsibility of the Director Corporate & Community Services to monitor the adequacy of this policy and implement and approve appropriate changes. This policy will be formally reviewed every four (4) years or as required by Council.