MANDATORY DATA BREACH NOTIFICATION POLICY

(STATUTORY POLICY)

1. Scope

The Mandatory Data Breach Notification Policy (this Policy) applies to all Council employees, contractors, Councillors, volunteers, work experience students and third-party service providers who handle personal information on behalf of Council.

2. Purpose

Livingstone Shire Council is committed to protecting personal information in accordance with the *Information Privacy Act 2009*. This Policy explains how Council will respond to, assess and manage actual, suspected and eligible data breaches under the Mandatory Notification of Data Breaches (MNDB) scheme in Chapter 3A of the *Information Privacy Act 2009*.

3. References (legislation/related documents)

Legislative reference

Information Privacy Act 2009
Information Privacy and Other Legislation Amendment Act 2023 (IPOLA)
Human Rights Act 2009
Public Records Act 2023
Right to Information Act 2009

Related documents

Mandatory Data Notification Breach Procedure
Mandatory Data Breach Response Plan

4. Definitions

To assist in interpretation, the following definitions shall apply:

Council	Livingstone Shire Council.
Data Breach	An incident where unauthorised access to, disclosure of, or loss of personal information held by Council, potentially causing harm.
Eligible Data Breach	Occurs under section 47 of the *Information Privacy Act 2009* where: 1) there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or 2) there has been loss of personal information held by an agency that is likely to result in unauthorised access to, or

	unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.
Personal Information	As defined in section 12 of the *Information Privacy Act 2009*: 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	Serious harm occurs where the harm caused by the data breach has resulted, or may result, in a real and substantial detrimental effect to an individual, it includes serious physical, psychological, emotional, financial or reputational harm to an individual because of the access or disclosure. Other forms of harm can also meet the serious threshold.

5. Policy Statement

5.1 Council's Obligation

Council will:

- Take reasonable steps to contain and mitigate any data breach as soon as practicable.
- Assess a suspected breach within 30 days to determine whether it is an Eligible Data Breaches.
- Notify the Office of the Information Commissioner (OIC) and affected individuals when an Eligible Data Breach occurs.
- Maintain a confidential register of all suspected data breaches, assessed data breaches and Eligible Data Breaches; and
- Undertaken periodic reviews of the Data Breach Register to ensure there are clear arrangements to contain, mitigate, assess, and respond to data breaches in a timely way, and ultimately prevent reoccurrence.

5.2 Responding to a Data Breach

Council's Mandatory Data Breach Notification Procedure outlines the operational requirements, responsibilities, assessment processes, notification requirements and remediation activities undertaken in response to actual and suspected data breaches.

5.3 Notification

Where an Eligible Data Breach is identified, Council will notify:

- The Queensland Information Commissioner; and
- Affected individuals, unless an exception under the *Information Privacy Act 2009* applies.

Where direct notification to affected individuals is not practicable or achievable, Council will publish a notification on its website and take any other steps required under the Information Privacy Act 2009. The notification will remain publicly available for at least 12 months. Council is not required to notify affected individuals or the Information Commissioner where an exemption under Chapter 3A of the Information Privacy Act 2009 applies, including where remedial action has been taken and the data breach is no longer likely to result in serious harm.

5.4 Prevention and Training

Regular training will be provided to employees regarding data protection and breach response procedures.

5.5 Complaints

If an individual is not satisfied with the way council has managed an actual or suspected data breach involving their personal information, including council's assessment of the breach, notification decision, response actions or communication with affected individuals, they may lodge a formal complaint under council's Administrative Action Complaints Policy.

6. Changes to this Policy

This policy will be reviewed every two years, or earlier if required by legislative change or following a significant data breach.

7. Repeals/Amendments

Version	Date	Action
1.0	Initial Policy	Initial Policy relating to Mandatory Data Breach Notification Scheme effective from 1 July 2026. Approved by Council at meeting held 26 October 2026.

THOMAS UPTON
CHIEF EXECUTIVE OFFICER