

Data Breach Policy

Effective Date	<i>1 July 2026</i>
Policy Type	<i>Statutory Policy</i>
Policy Owner	<i>ICT Manager</i>
Link to Corporate Plan	<i>Sustainable Organisation</i>
Review Date	<i>1 July 2028</i>
Related Legislation	<i>Information Privacy Act 2009</i>
Related Documents	<i>Western Downs Regional Council Data Breach Response Plan</i>

Policy Version	Approval Date	Adopted/Approved
<i>1</i>	<i>21/05/2026</i>	<i>Adopted Ordinary Meeting of Council</i>

*This policy may not be current as Council regularly reviews and updates its policies. The latest controlled version can be found in the policies section of Council's intranet or Website. **A hard copy of this electronic document is uncontrolled.***



Data Breach Policy

1. PURPOSE

The purpose of this policy is to ensure that Council manages the notification of data breaches in accordance with the *Information Privacy Act 2009*.

2. SCOPE

This policy applies to any data breach that occurs for personal information held by Council.

3. POLICY

3.1 Principles

Council is committed to protecting the privacy of individuals and safeguarding all personal information which is collected, stored, or transmitted by Council, whether paper based or electronic.

'Data Breach' is defined in Schedule One of the *Information Privacy Act 2009*. Practically, a data breach occurs when there is unauthorised access, disclosure, or loss of personal information held by Council.

When the unauthorised access to or disclosure of personal information is likely to result in serious harm to an individual to whom the personal information relates, the data breach will be classified as an eligible data breach and will be subject to the mandatory notification of data breaches provisions of the *Information Privacy Act 2009*.

3.2 Provisions

Council will manage any data breach in accordance with the regime prescribed by Chapter 3A, Mandatory notification of data breaches, of the *Information Privacy Act 2009*.

