Data Management Policy

1 Policy Purpose

This Policy sets out Council's commitment to the effective, lawful, and secure management of data across its entire lifecycle. It establishes the principles that govern how Council data is collected, stored, accessed, shared, retained, and disposed of.

This policy gives effect to the Data Management Administrative Policy. Operational requirements, procedures, and specific obligations for Personnel are set out in the Data Management Administrative Policy, which is to be read alongside this document.

2 Policy Scope

This Policy applies to:

- All Council elected members, employees, contractors, consultants, volunteers, agents and third-party service providers who create, access, use, store, share, or dispose of Council data in any form.
- It applies to all data held in Council ICT systems and devices, and to data held by third parties on Council's behalf, including business systems, cloud services, mobile devices, CCTV systems, and backup repositories.

3 Policy Statement

3.1 Council's Commitment

Data is one of Council's most important assets. It underpins service delivery, lawful decision-making, financial management, and accountability to the community. Much of the data Council holds relates to individuals, residents, ratepayers, employees, and service users, who have a legitimate expectation that their information will be handled with care, lawfulness, and respect for their privacy.

Council is committed to managing its data in a way that protects confidentiality, maintains integrity, and supports availability across the full data lifecycle, while meeting all legal, privacy, and recordkeeping obligations.

Council is committed to complying with the Information Privacy Act 2009 (Qld) as amended by the Information Privacy and Other Legislation Amendment Act 2023 (Qld), the Public Records Act 2023 (Qld), and all other applicable legislation governing the collection, use, disclosure, and retention of data. Council notes that the Mandatory Notification of Data Breach (MNDB) scheme introduced by the Information Privacy and Other Legislation Amendment Act 2023 (Qld) will apply to local governments from 1 July 2026, and is committed to ensuring it is prepared to meet those obligations on commencement.

Council expects all Personnel and third-party providers to understand and take seriously their data management responsibilities, and to treat the data they handle with the same care and professionalism they would wish applied to their own personal information.

3.2 GOVERNING PRINCIPLES

3.2.1 Lawful and ethical data handling.

Council data must be collected, used, and disclosed only for lawful, legitimate Council purposes. Personal information must be handled in accordance with the Queensland Privacy Principles under the Information Privacy Act 2009 (Qld). Data must not be collected in excess of what is reasonably necessary for the purpose.

3.2.2 Data classification and proportionate protection.

All Council data must be classified according to its sensitivity and criticality:

- **Public.** Information approved for unrestricted public access.
- **Internal**. Information intended for use within Council that does not contain personal information or commercially sensitive material.
- **Confidential**. Information that, if disclosed, could cause harm to individuals or Council. Includes personal information, commercially sensitive material, and operational security information.
- **Highly Confidential.** Information requiring the highest level of protection. Includes sensitive personal information, legal privilege material, and information the disclosure of which could cause serious harm.

3.2.3 Confidentiality, integrity, and availability

Council data must be protected from unauthorised access, disclosure, modification, and loss. Data must be accurate, complete, and available to authorised users when needed. Controls must be maintained across the full lifecycle of the data, from creation through to secure disposal.

3.2.4 Least privilege access.

Access to Council data must be granted only to Personnel who require it to perform their duties, and must be limited to the minimum necessary for that purpose. Access rights must be reviewed regularly and revoked when no longer required.

3.2.5 Data sovereignty and approved storage.

In accordance with the Queensland Privacy Principles, Council data must be stored and processed within Australia unless the Chief Executive Officer has expressly approved an exception and appropriate safeguards are in place. Personnel must not store or transmit Council data using unapproved personal, cloud, or consumer services.

3.2.6 Retention, disposal, and records obligations.

Council data must be retained for as long as required by law, regulation, or business need, and in accordance with applicable Queensland State Archives retention and disposal schedules. Data no longer required must be disposed of securely using approved methods. As a public body, Council's data management practices are subject to the Public Records Act 2023 (Qld).

3.2.7 Privacy by design and data minimisation.

Privacy and data protection considerations must be built into Council systems, processes, and projects from the outset. Where possible, personal data should be anonymised or pseudonymised. Data collection must be limited to what is reasonably necessary for the legitimate purpose.

3.2.8 Breach identification, notification, and response.

Council must have in place effective mechanisms to detect, assess, contain, and respond to data breaches. The Mandatory Notification of Data Breach (MNDB) scheme under the Information Privacy and Other Legislation Amendment Act 2023 (Qld) will apply to local governments from 1 July 2026. Council is committed to preparing for those obligations ahead of commencement, including by ensuring it has a data breach policy, breach register, and response procedures in place.

3.2.9 Accountability and continuous improvement.

Council must be able to demonstrate compliance with its data management obligations. Data handling records, audit evidence, and breach notifications must be maintained. Data management controls must be reviewed periodically to identify improvement opportunities and address recurring incidents or data quality issues.

5 Human Rights Compatibility Statement

This policy has been assessed as compatible with human rights pursuant to the *Human Rights Act 2019* (Qld).

6 Definitions

Term	Definition
Council	Pormpuraaw Aboriginal Shire Council
Data	Information in any form, including records, documents, images, audio, video, spreadsheets, databases, and system logs, whether structured or unstructured, digital or physical.
Data breach	An incident involving unauthorised access to, disclosure of, loss of, or damage to personal information or other Confidential or Highly Confidential data.
Data classification	The category assigned to data based on its sensitivity and criticality, used to determine appropriate handling, access, storage, and disposal requirements. Classification levels are set out in the ICT Information Security Strategic Policy.
Data sovereignty	The principle that data is subject to the laws and governance requirements of the jurisdiction in which it is collected, stored, or processed.
Eligible data breach	A data breach that is required to be notified to the relevant authority and affected individuals under the Information Privacy and Other Legislation Amendment Act 2023 (Qld) because it is likely to result in serious harm to one or more affected individuals.
ICT	Information, Communications and Technology.
ICT systems	All hardware, software, networks, cloud services, mobile devices, communication tools, and information systems owned, leased, or operated by Council.
Mandatory Notification of Data Breach (MNDB) scheme	The data breach notification scheme established by the Information Privacy and Other Legislation Amendment Act 2023 (Qld), applicable to local governments from 1 July 2026.

Term	Definition
Personal information	Has the meaning given in the Information Privacy Act 2009 (Qld).
Personnel	All elected members, employees, contractors, volunteers, consultants, and agents of Council.
Public record	Has the meaning given in the Public Records Act 2023 (Qld).
Queensland Privacy Principles (QPPs)	The privacy principles set out in the Information Privacy Act 2009 (Qld) that govern how agencies collect, store, use, and disclose personal information.
Retention and disposal schedule	A Queensland State Archives approved schedule specifying how long Council records must be kept and how they must be disposed of when no longer required.

7 Related Policies and Other Documents

Legislation:
Local Government Act 2009 (Qld)
Local Government Regulation 2012 (Qld)
Information Privacy Act 2009 (Qld)
Information Privacy and Other Legislation Amendment Act 2023 (Qld)
Public Records Act 2023 (Qld)
Cyber Security Act 2024 (Cth)

Associated Documents:
Data Management Administrative Policy
ICT Equipment Acceptable Use Strategic Policy
ICT Information Security Strategic Policy
ICT Incident Response Strategic Policy
Records Management Policy
Code of Conduct
Councillor Code of Conduct

8 Monitoring and Review

This policy is to be reviewed every four (4) year for relevance and to ensure that its effectiveness is maintained.

9 Responsibility

This Policy is to be implemented by the CEO; and reviewed and amended in accordance by the Governance and Records Officer.

10 Version Control

Version	Details	Resolution No	Date
V1	Created and adopted	2026/46	25 March 2026