Data Breach Policy

1 Head of Power

- *Information Privacy Act 2009*

2 Policy Purpose

This policy sets out how Council will prepare for, identify, contain, assess, notify and review data breaches, including Eligible Data Breaches, in accordance with the Information Privacy Act 2009 (Qld) (IP Act) and the Mandatory Notification of Data Breach (MNDB) scheme.

The MNDB scheme applies to local government from 1 July 2026. From that date, Council must take prescribed actions in responding to a data breach, including:

a) immediately taking all reasonable steps to contain and mitigate the data breach;

b) if Council does not know whether the data breach is an Eligible Data Breach, assessing within thirty (30) days whether there are reasonable grounds to believe the data breach is an Eligible Data Breach;

c) notifying other affected agencies; and

d) if Council knows or assesses the data breach as an Eligible Data Breach, notifying the Office of the Information Commissioner (OIC) and the individuals whose personal information is the subject of the breach, unless an exemption to notification applies.

The MNDB scheme also requires Council to prepare and publish this Data Breach Policy on an accessible Council website (section 73 of the IP Act).

As this is a Statutory Policy, it operates as a combined policy and procedure.

3 Policy Scope

This Policy applies to:

- All elected members, employees, contractors, volunteers, consultants and agents of Council.
- It applies to all personal information and other information held by Council, whether in electronic or physical form.
- It extends to third party service providers, including Contracted Service Providers, where they hold personal information on behalf of Council or where a data breach by the third party may affect personal information for which Council is responsible.

4 POLICY STATEMENT

4.1 ROLES AND RESPONSIBILITIES

All Personnel	• Read and understand this Data Breach Policy and any Data Breach Response Plan. • Comply with the IP Act, including protecting personal information held by Council from unauthorised access, disclosure or loss. • Immediately report any actual or suspected data breach to their supervisor, manager or the Responsible Manager. • Cooperate with the Responsible Manager and/or the Data Breach Response Team in responding to a data breach. • Comply with recordkeeping obligations.
Responsible Manager (Privacy Officer or equivalent)	• Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm. • Escalate medium and high risk data breaches to the Chief Executive Officer. • Coordinate notification to the Information Commissioner, affected individuals and other parties where required, including publishing, monitoring and reviewing the currency of public notifications published to Council's website under section 53(1)(c). • Where a data breach is also a cyber security incident, immediately report to the ICT Manager (or equivalent) if not already reported, and coordinate to ensure both privacy and cybersecurity response requirements are met. • Maintain the Register of Eligible Data Breaches. • Oversee the post-breach review and remediation process. • Maintain and update this policy.
Manager	• Identify and escalate concerns within area of responsibility which may enliven the requirements of this policy. • Where a data breach is also a cyber security incident, immediately report to the Responsible Manager if not already reported.

Chief Executive Officer	• Has overall accountability for Council's compliance with the MNDB scheme. • Convene the Data Breach Response Team when required. • Approve notification to the Information Commissioner and affected individuals for Eligible Data Breaches. • Ensure sufficient resources are allocated to data breach preparedness and response. • Ensure this policy is published on Council's website. • Implement relevant cyber security management plans and related procedures where the data breach is also a cyber security incident.
Data Breach Response Team	• Manage a data breach that is assessed as medium or high risk, including where the breach is likely to cause serious harm to any affected individual or to Council's systems. • Oversee containment, assessment, notification and post-breach review for serious data breaches. • Membership is determined by the nature of the breach and may include representatives from privacy, ICT, cybersecurity, communications, human resources and legal functions. • Subject matter expert teams may be co-opted depending on the source and nature of the data breach.

4.2 Responding to a Data Breach

Council's response to a data breach follows six stages. The nature and extent of the response at each stage will be proportionate to the severity and scale of the data breach.

4.2.1 Stage 1: Preparation

Council will maintain the following preparedness measures to support an effective response to a data breach:

a) This Data Breach Policy will be published on Council's website and made available to all Personnel.

b) Council will maintain relevant technical and organisational controls for identifying and detecting data breaches, as set out in the ICT Information Security Administrative Policy. These controls will include measures designed to prevent data breaches caused by human error (such as delayed sending of emails and access controls on bulk data), recognising that human error is typically the most common cause of data breaches.

c) Council will ensure Personnel receive security awareness training that includes how to identify and report a data breach, consistent with the ICT Security Awareness Administrative Policy.

d) Council will maintain contact details for the OIC, the Australian Information Commissioner (where relevant), and any external cyber incident response or legal service providers that may need to be engaged.

e) This policy will be tested and reviewed at least annually to ensure it remains current and effective. Testing may include tabletop exercises simulating data breach scenarios relevant to Council's operations.

f) Council will ensure its contracts with Contracted Service Providers include requirements for prompt notification to Council of any data breach affecting personal information held on Council's behalf, together with defined roles and responsibilities for assessment, remediation, information flow and notification.

g) This policy interacts with Council's broader systems, policies and procedures, including cyber incident response procedures, general incident and emergency management processes, communications strategies, and fraud and corruption prevention frameworks. Where a data breach also constitutes a cyber security incident, both this policy and any applicable cyber incident response procedures will be engaged concurrently.

4.2.2 Stage 2: Identification

A data breach may be identified through a range of internal and external sources, including Personnel reports, automated system alerts, reports from members of the public, notification from another agency, or notification from a Contracted Service Provider.

Not every data breach will be an Eligible Data Breach. A data breach can result from malicious external actions (such as a cyber-attack), internal human error (such as sending personal information to the wrong recipient, misplacing a physical file, or failing to redact personal information before publication), or a failure of systems or processes. Council should assume that human errors will be the most common cause of data breaches and should design systems and processes accordingly. An Eligible Data Breach always involves personal information and is likely to result in serious harm.

When a data breach is identified or suspected, Personnel must:

a) Immediately report the breach to their supervisor or the Responsible Manager.

b) Record the date and time the breach was identified, the nature of the information involved, how the breach occurred (if known), and the actions taken.

c) Not attempt to investigate the breach independently.

The Responsible Manager will undertake an initial evaluation to determine the nature and scope of the breach, whether personal information is involved, and the appropriate risk level.

4.2.2.1 Activation of the Data Breach Response Team

a) The Data Breach Response Team will be convened by the Chief Executive Officer (or delegate) where the initial evaluation indicates that a data breach is medium or high risk. Examples of circumstances that would typically warrant activation include:

i) A cyber-attack or ransomware incident affecting Council systems that store personal information.

ii) Unauthorised access to, or disclosure of, sensitive personal information such as health information, financial information, TFNs, or information relating to vulnerable persons (including children or domestic violence victim-survivors).

iii) A data breach affecting a large number of individuals.

iv) Loss or theft of an unencrypted device containing personal information.

v) A data breach that has attracted, or is likely to attract, public or media attention.

vi) A data breach that may also constitute a notifiable cyber security incident under the Cyber Security Act 2024 (Cth).

b) For lower-risk breaches (for example, a misdirected email to a single known recipient who has confirmed deletion), the Responsible Manager may manage the response without convening the Data Breach Response Team.

4.2.3 Stage 3: Containment and Mitigation

Upon becoming aware of a data breach, Council must immediately take all reasonable steps to contain the breach and mitigate any resulting harm. The specific containment and mitigation measures will depend on the nature and severity of the breach, but may include:

h) Disabling or isolating compromised accounts, systems or devices.

i) Changing access credentials, including passwords and access codes.

j) Recovering personal information where possible, including contacting any person who may have received information in error.

k) Stopping the activity that led to the breach, or shutting down the affected system.

l) Engaging internal ICT and cybersecurity resources, or external incident response providers where required.

m) Preserving evidence for investigation purposes.

4.2.3.1 Risk assessment

The Responsible Manager (or the Data Breach Response Team, if convened) must conduct a risk assessment to inform containment and mitigation strategies and to determine whether the breach may be an Eligible Data Breach. The following framework must guide the risk assessment:

Factor	Guidance
Nature and sensitivity of information	If the data breach involved sensitive information (for example, health data, financial data, TFNs, identity documents, or information about vulnerable individuals), the risk of harm to affected individuals is higher. Consider whether the information was already publicly accessible. Information that is not publicly available poses a greater risk when breached. Linked personal information (for example, health data combined with identity information) poses a greater risk than isolated personal information, as it can enable identity theft or other serious crimes.
Amount of information and number of affected individuals	Consider the total volume of information affected and the total number of individuals whose personal information has been affected. The more data and individuals affected, the higher the risk.
Ease of identifying individuals	Consider how easy it is for a person with access to the information to identify an individual, whether directly or by combining the information with other available data. Information that directly identifies individuals poses a higher risk.
Seriousness of the harm	Consider the potential harm to individuals, including physical harm, psychological stress, humiliation, reputational damage, financial loss, and identity fraud. If the breach concerns personal information of vulnerable individuals (for example, children, elderly persons, or domestic violence victim-survivors), a higher risk of harm may be attributed.
Existing mitigating measures	Consider whether any existing security measures (for example, encryption, access controls, or remote wipe capabilities) were in place at the time of the breach and how effectively they protect the affected individuals. Consider whether containment actions have reduced the risk (for example, the unauthorised recipient has confirmed deletion of the information).

4.2.3.2 Risk tiering

Based on the risk assessment, each data breach must be classified as low, medium or high risk. The risk level determines the response approach:

Risk Level	Indicators	Response Approach
Low	• Small scale / minor breach • Non-sensitive information • Single known recipient who confirms deletion • No personal information involved, or personal information unlikely to result in harm	• Managed by Responsible Manager • Containment and mitigation • Record in breach register • Post-breach review • MNDB notification not required
Medium	• Personal information involved • More than one individual affected • Possible but uncertain risk of serious harm • Suspected Eligible Data Breach	• Data Breach Response Team convened • Formal 30-day assessment under s.48(2)(b) • Containment, mitigation and evidence preservation • Determine whether notification required • Escalation to CEO
High	• Sensitive or linked personal information • Large number of individuals affected • Likely serious harm • Eligible Data Breach confirmed or highly likely • Cyber-attack, ransomware, or systemic compromise	• Data Breach Response Team convened immediately • Senior executive involvement • Immediate containment • Expedited assessment and notification • External expertise engaged as required • Communications strategy activated

4.2.4 Stage 4: Assessment

Where Council has reasonable grounds to suspect that a data breach may be an Eligible Data Breach but does not have sufficient information to form a reasonable belief, Council must carry out an assessment within thirty (30) days to determine whether there are reasonable grounds to believe the data breach is an Eligible Data Breach (section 48(2)(b) of the IP Act).

If Council is satisfied it will be unable to complete the assessment within 30 days, the assessment period may be extended in accordance with section 49 of the IP Act.

In carrying out the assessment, Council must consider the following factors prescribed under section 47(2) of the IP Act:

a) The kind of personal information that has been accessed, disclosed or lost.

b) The sensitivity of the personal information.

c) Whether the personal information is protected by one or more security measures.

d) If the personal information is protected by security measures, the likelihood that any of those measures could be overcome.

e) The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information.

f) The nature of the harm likely to result from the data breach.

g) Any other relevant matter.

Other relevant matters may include but are not limited to:

a) The nature and cause of the breach (including whether a counterparty or third party caused the breach).

b) Whether the breach has affected another agency.

c) Any vulnerabilities of affected individuals, for example where children, elderly persons, or domestic violence victim-survivors are involved.

d) The effectiveness of the steps taken to contain and mitigate the breach.

e) Whether the personal information was collected by Council or by another entity.

f) Whether a reasonable person would conclude the breach is likely to result in serious harm.

The assessment must be documented, including the information considered, the conclusion reached, and the reasons for the conclusion. Council may engage external experts to assist with the assessment of a complex data breach.

Where the assessment determines the data breach is an Eligible Data Breach, Council must proceed to the notification stage.

4.2.5 Stage 5: Notification

4.2.5.1 Notification to the Information Commissioner

Unless an exemption under the IP Act applies, Council must notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an Eligible Data Breach.

Notification must be made in writing and must include a statement prepared under section 51 of the IP Act.

Council may seek advice from the OIC about a data breach at any time, but formal notification of an Eligible Data Breach must be made in writing.

4.2.5.2 Notification to affected individuals

Unless an exemption applies, Council must, as soon as practicable after forming a reasonable belief that a data breach is an Eligible Data Breach, take reasonable steps to notify affected individuals in accordance with section 53 of the IP Act. Council must use the following approach:

i) Option 1: If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, Council must take reasonable steps to notify each individual directly (by telephone, letter, email or in person).

ii) Option 2: If Option 1 does not apply, Council must take reasonable steps to notify each affected individual (that is, each individual who is likely to suffer serious harm) of the required information, if reasonably practicable.

iii) Option 3: If Council cannot directly notify individuals under Option 1 or Option 2, Council must publish the required information on its website for a period of at least twelve (12) months (section 53(1)(c) of the IP Act) and advise the Information Commissioner how to access the notice. The Information Commissioner is required to publish the notice on the Commissioner's website for at least 12 months.

Council must ensure it has sufficient information about the breach before issuing notifications. Premature notifications are not recommended and may cause unnecessary harm, panic and concern.

4.2.5.3 Content of notification to individuals

To the extent reasonably practicable, notification to individuals must include the information set out in section 53(2) of the IP Act:

iv) The date the breach occurred.

v) A description of the breach.

vi) How the breach occurred.

vii) The personal information included in the breach.

viii) The period of time the personal information was disclosed for.

ix) Actions taken or planned to secure the information or control and mitigate harm.

x) Recommendations about steps the individual should take in response.

xi) Information about complaints and reviews of agency conduct.

xii) The name of the agencies subject to the breach.

xiii) Contact details for Council or the nominated contact person.

Council is not required to include information in its notice if doing so would prejudice its functions.

4.2.5.4 Notification to other agencies

Where a data breach affects another agency, Council must notify that agency and coordinate the response, including notification to affected individuals, in accordance with sections 50 and 54 of the IP Act.

Council will maintain documented key contacts and defined roles and responsibilities for managing multi-agency breaches, including responsibilities for assessment, remediation, information flow and notification to individuals and the Information Commissioner.

Where a disclosing agency makes an inquiry under section 54 of the IP Act about how Council has managed a breach affecting information disclosed by that agency, Council must respond to the inquiry.

4.2.5.5 Voluntary notification

g) Even where notification is not mandatory under the IP Act (for example, where the breach does not meet the threshold for an Eligible Data Breach), Council may elect to voluntarily notify affected individuals where it considers notification is appropriate in the circumstances. This may be appropriate where the public would be unlikely to accept a technical argument as to why Council was not required to notify.

4.2.5.6 Exemptions from notification

h) Council will determine whether any exemption to the notification requirements applies under the IP Act before deciding not to notify. Where an exemption is relied upon, the reason must be documented.

4.2.5.7 Communications strategy

i) For medium and high risk data breaches, the Responsible Manager (or the Data Breach Response Team) must develop a communications strategy that addresses:

   i) Internal communications to relevant Personnel, senior management and the elected Council, as appropriate to the severity of the breach.

   ii) External communications with affected individuals beyond the statutory notification, including establishing a dedicated point of contact or helpline for inquiries.

   iii) Media management, including preparation of holding statements, designation of a spokesperson, and protocols for responding to media inquiries.

   iv) Communications with external stakeholders, Contracted Service Providers, insurers and other third parties who may be affected by or involved in responding to the breach.

   v) Coordination of communications with any other affected agency.

j) The communications strategy must be proportionate to the nature and scale of the breach. For lower-risk breaches, a formal communications strategy may not be required.

4.2.6 Stage 6: Post-Breach Review and Remediation

After a data breach has been managed, Council must undertake a post-breach review and remediation process. The nature and depth of the review will be proportionate to the severity of the breach.

The review must:

a) Analyse all aspects of the data breach, including its cause (with particular attention to whether human error contributed), the effectiveness of the response, and the adequacy of containment and mitigation measures.

b) Identify key learnings and any changes required to prevent recurrence or reduce the risk of similar breaches.

c) Consider whether updates are needed to this policy, any Data Breach Response Plan, related policies, procedures, systems, or technical controls.

d) Consider whether additional training or awareness activities are required for Personnel.

e) Assess the effectiveness of the Data Breach Policy itself and whether the response processes operated as intended.

Responsibility for the post-breach review will depend on the nature and scale of the breach. Where a Data Breach Response Team has been convened, the team will conduct the review. For lower-risk breaches, the Responsible Manager will conduct the review.

The results of the post-breach review must be documented and reported to the Chief Executive Officer. Responsibility for actioning the learnings and monitoring the implementation of remediation activities must be clearly allocated.

4.2.6.1 Register of Eligible Data Breaches

Council must maintain a Register of Eligible Data Breaches in accordance with section 55 of the IP Act.

The Register must record, for each Eligible Data Breach: the date the breach occurred; the date the breach was identified; a description of the breach; the personal information involved; the number of affected individuals (if known); the actions taken to contain and mitigate the breach; the assessment outcome; the notifications given (including dates and methods); and the outcome of any post-breach review.

The Register must be made available for inspection by the Information Commissioner upon request.

4.2.6.2 Recordkeeping

All records relating to a data breach response, including reports, assessments, decisions, notifications, minutes of meetings and the Register of Eligible Data Breaches, must be managed in accordance with the Public Records Act 2023 (Qld).

A single repository of information must be maintained to document each data breach and the response, including all key decision-making records. This will ensure consistency with Council's recordkeeping obligations and support any subsequent review or audit.

4.2.6.3 Training and Awareness

All Personnel must receive training on this policy as part of induction, and at least annually thereafter, consistent with the ICT Security Awareness Administrative Policy.

Training must include what constitutes a data breach and an Eligible Data Breach; common causes of data breaches including human error; how to recognise and report a data breach; the distinction between a data breach and an Eligible Data Breach; Personnel's obligations under this policy; and Council's notification obligations under the MNDB scheme.

4.2.7 Publication

This policy must be published on Council's website in accordance with section 73 of the IP Act. The published version must be kept current and updated whenever a material amendment is made.

5 HUMAN RIGHTS COMPATIBILITY STATEMENT

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

6 DEFINITIONS

Term	Definition
Affected individual	An individual to whom personal information the subject of an Eligible Data Breach relates, who is likely to suffer serious harm as a result of the data breach (section 47(1) of the IP Act).
Agency worker	A person who carries out work in any capacity for Council, including employees, contractors, subcontractors, apprentices, trainees, students gaining work experience, and volunteers.
Australian Information Commissioner	The Australian Information Commissioner appointed under the Australian Information Commissioner Act 2010 (Cth).
Commonwealth Privacy Act	The Privacy Act 1988 (Cth).
Contracted Service Provider	A service provider bound by a contractual arrangement with Council under which the provider is required to comply with the Queensland Privacy Principles in relation to personal information handled for Council.
Council	Pormpuraaw Aboriginal Shire Council.
Data breach	The unauthorised access to, or unauthorised disclosure of, information held by Council, or the loss of information held by Council where unauthorised access to, or unauthorised disclosure of, the information is likely to occur (Schedule 5 of the IP Act).
Data Breach Policy	This policy.
Data Breach Response Plan	A more detailed procedural document, which may be developed to complement this policy, setting out specific internal processes for managing and responding to a data breach.
Data Breach Response Team	The team convened by the Chief Executive Officer or delegate to manage a data breach that is assessed as medium or high risk. Membership may include representatives from privacy, ICT, cybersecurity, communications, human resources and legal functions, with senior executive involvement for serious breaches.
Eligible Data Breach	A data breach involving personal information held by Council where: (a) there has been unauthorised access to, or unauthorised disclosure of, personal information and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or (b) there has been loss of personal information that is likely to result in unauthorised access or disclosure, and the loss is likely to result in serious harm to any of the individuals to whom the information relates (section 47 of the IP Act).

Term	Definition
Held (or hold) in relation to personal information	Personal information is held by Council if the personal information is contained in a document in the possession, or under the control, of Council.
Information Commissioner	The Queensland Information Commissioner.
IP Act	The Information Privacy Act 2009 (Qld).
MNDB scheme	The Mandatory Notification of Data Breach scheme established under Chapter 3A of the IP Act.
OIC	The Office of the Information Commissioner (Queensland).
Personal information	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 (Schedule 5 of the IP Act).
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).
Register of Eligible Data Breaches	The register maintained by Council recording all Eligible Data Breaches in accordance with section 55 of the IP Act.
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 (section 47(3) of the IP Act).
Suspected Eligible Data Breach	A data breach that Council reasonably suspects may be an Eligible Data Breach, but for which Council has not yet formed a reasonable belief (section 48(2)(b) of the IP Act).
TFN	A tax file number, being a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.

7 Related Policies and Other Documents

Legislation:
Information Privacy Act 2009 (Qld)
Information Privacy and Other Legislation Amendment Act 2023 (Qld)
Local Government Act 2009 (Qld)
Local Government Regulation 2012 (Qld)
Public Records Act 2023 (Qld)
Human Rights Act 2019 (Qld)
Cyber Security Act 2024 (Cth)

Associated Documents:
ICT Information Security Strategic Policy
ICT Information Security Administrative Policy
ICT Password Security Strategic Policy
ICT User Access Management Strategic Policy
ICT Security Awareness Strategic Policy
Code of Conduct
Councillor Code of Conduct

8 Monitoring and Review

Notwithstanding the above, this policy is to be reviewed every four (4) years 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 by the Governance and Records Officer.

10 Version Control

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