Kowanyama Aboriginal Shire Council

Information Privacy Policy

Policy Number:	KASC-STRAT-038
Responsible Manager:	Executive Manager Corporate and Financial Services
Legislation:	Local Government Act 2009 Local Government Regulation 2012 Public Records Act 2002 Right to Information Act 2009 Privacy Act 1988 Information Privacy Act 2009 Crime and Corruption Act 2001 Electronic Transactions (Queensland) Act 2001 Public Interest Disclosure Act 2010
Associated Documents:	Right to Information Policy Information, Communication and Technology (ICT)
Approval Date:	26 May 2026

1. Purpose

This policy sets out how Council will comply with its obligations under the Information Privacy Act 2009 (Qld) (IP Act) to protect the personal information it holds. It establishes Council's commitment to managing personal information in accordance with the Queensland Privacy Principles (QPPs) and describes how Council will collect, hold, use, disclose and otherwise handle personal information.

The QPPs commenced on 1 July 2025, replacing the former Information Privacy Principles (IPPs) and National Privacy Principles (NPPs). The Mandatory Notification of Data Breach (MNDB) scheme applies to local government from 1 July 2026.

Under QPP 1, Council must have a clearly expressed and up-to-date privacy policy that explains how it manages personal information. This policy fulfils that obligation.

As this is a Statutory Policy, it operates as a combined policy and procedure. It goes beyond what is normally required in a policy as it needs to meet the requirements detailed in the relevant legislation. This policy must be published on Council's website, made available free of charge and in an appropriate form.

2. Scope

This policy applies to all elected Members, employees, contractors, volunteers, consultants and agents of Council.

It applies to all personal information held by Council, whether in electronic or physical form, including personal information collected before the commencement of the IP Act.

It extends to Contracted Service Providers who are bound to comply with the QPPs in relation to personal information handled on Council's behalf.

3. Terms and Definitions

In this policy:

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 breach (section 47(1) of the IP Act).
Contracted Service Provider	A service provider bound by a contractual arrangement with Council under which the provider is required to comply with the QPPs in relation to personal information handled for Council.
Council	Kowanyama 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 or disclosure is likely to occur (Schedule 5 of the IP Act).
Eligible Data Breach	Has the meaning given in section 47 of the IP Act.
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, whether the information or opinion is true or not and whether 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.
QPPs	The Queensland Privacy Principles set out in Schedule 3 of the IP Act.
QPP privacy policy	This policy, being the privacy policy required under QPP 1.
Sensitive information	Personal information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, criminal record, health information, or genetic or biometric information.

4. Roles and responsibilities

All Personnel	• Read and understand this policy. • Comply with the QPPs and this policy in all dealings with personal information. • Collect, use and disclose personal information only for authorised purposes. • Report any actual or suspected data breach immediately in accordance with the Data Breach Statutory Policy. • Complete privacy training as required. • Immediately report any actual or suspected non-compliance to their supervisor, manager or the Responsible Manager. • Cooperate with any investigation or response activity under this policy. • Comply with recordkeeping obligations.
Manager	• Identify and escalate concerns within area of responsibility which may enliven the requirements of this policy. • Ensure Personnel within their area of responsibility are aware of and comply with this policy.
Responsible Manager (Privacy Officer or equivalent)	• Oversee Council's compliance with the IP Act and the QPPs. • Maintain and update this policy. • Manage privacy complaints and enquiries. • Coordinate data breach responses in accordance with the Data Breach Statutory Policy. • Ensure Personnel receive privacy training. • Report to the Chief Executive Officer on privacy compliance. • Oversee review and remediation processes.
Chief Executive Officer	• Has overall accountability for Council's compliance with the legislative requirements underpinning this policy. • Ensure sufficient resources are allocated to privacy management. • Ensure this policy is published on Council's website.

5. Policy

5.1. Council's commitment

Council recognises that privacy is a fundamental human right. Section 25 of the Human Rights Act 2019 (Qld) provides that a person has the right not to have their privacy unlawfully or arbitrarily interfered with. Council will act compatibly with this right in all its functions and activities.

Council is committed to protecting the privacy of individuals whose personal information it holds. Council will:

a) Comply with the QPPs and any QPP codes approved under the IP Act.

b) Manage personal information in an open and transparent way.

c) Collect only the personal information that is reasonably necessary for, or directly related to, Council's functions and activities.

d) Take reasonable steps to ensure personal information is accurate, up-to-date, complete, relevant and not misleading.

e) Protect personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

f) Comply with the MNDB scheme from 1 July 2026, in accordance with the Data Breach Statutory Policy.

g) Provide individuals with access to their personal information and the ability to request correction, in accordance with the Right to Information Act 2009 (Qld).

h) Ensure Personnel receive appropriate training on their privacy obligations.

5.2. Queensland Privacy Principles

Council must comply with the following QPPs in its handling of personal information:

1. **QPP 1 — Open and transparent management of personal information**
   - Council must take reasonable steps to implement practices, procedures and systems to ensure compliance with the QPPs and to enable it to deal with inquiries or complaints about its privacy practices.
   - Council must maintain this QPP privacy policy in a clearly expressed, up-to-date form and make it available free of charge.
   - In addition to this policy, Council will maintain a publicly accessible privacy statement on its website that provides plain-language information about what personal information Council collects, how it is collected, how it is used and disclosed, how it is secured, and how individuals can access and correct their personal information.

2. **QPP 2 — Anonymity and pseudonymity**
   - Where it is lawful and practicable, individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with Council.

3. **QPP 3 — Collection of solicited personal information**
   - Council must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of Council's functions or activities.
   - Council must collect personal information only by lawful and fair means and must collect information directly from the individual unless it is unreasonable or impracticable to do so.
   - Sensitive information must not be collected unless the individual consents and the information is reasonably necessary for Council's functions, or collection is required or authorised by law.

4. **QPP 4 — Dealing with unsolicited personal information**
   - If Council receives personal information, it did not solicit, it must determine whether it could have collected the information under QPP 3. If it could not have, and the information is not a public record, Council must destroy or de-identify the information as soon as practicable.

5. **QPP 5 — Notification of the collection of personal information**
   - At or before the time of collecting personal information (or as soon as practicable afterwards), Council must take reasonable steps to notify the individual of matters including the purpose of collection, the consequences if information is not collected, and any usual disclosures of the information.

6. **QPP 6 — Use or disclosure of personal information**
   - Council must not use or disclose personal information for a purpose other than the purpose for which it was collected (the primary purpose), unless an exception under QPP 6 applies, including where the individual consents, the use or disclosure is required or authorised by law, or the individual would reasonably expect the secondary use or disclosure.

7. **QPP 10 — Quality of personal information**
   - Council must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose of use or disclosure.

8. **QPP 11 — Security of personal information**
   - Council must take reasonable steps to protect personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.
   - Council must take reasonable steps to destroy or de-identify personal information when it is no longer needed for any purpose for which the information may be used or disclosed, subject to the requirements of the Public Records Act 2023 (Qld).

9. **QPP 12 — Access to personal information**
   - On request, Council must give an individual access to personal information held about them, unless an exception applies. Applications for access are made under the Right to Information Act 2009 (Qld).

10. **QPP 13 — Correction of personal information**
    - Council must take reasonable steps to correct personal information it holds to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. Applications for amendment are made under the Right to Information Act 2009 (Qld).

5.3. How Council collects person information

5.3.1. Council collects personal information in a variety of ways while performing its functions and activities, including:

a) Directly from individuals when they complete application forms, make enquiries, lodge complaints, attend Council facilities, or interact with Council online.

b) From third parties, such as other government agencies, referees, or service providers, where it is unreasonable or impracticable to collect the information directly from the individual.

c) Through Council's ICT systems, including website analytics, CCTV systems and other monitoring systems where authorised.

5.3.2. Council will not collect personal information by unlawful or unfair means.

5.4. How Council uses and discloses personal information

5.4.1. Council uses personal information for the purposes for which it was collected, including (for example) providing services, processing applications, managing rates and charges, managing employees and contractors, responding to enquiries, and meeting its legislative obligations.

5.4.2. Council may disclose personal information to third parties where the disclosure is authorised under QPP 6, including to other government agencies, law enforcement, professional advisers, and Contracted Service Providers who perform services on Council's behalf.

5.4.3. Council does not sell or trade personal information. Where Council discloses personal information to overseas recipients, it does so in accordance with the requirements of section 33 of the IP Act and the overseas disclosure requirements set out in section 6.7 of this policy.

5.4.4. Council may disclose work-related personal information of Personnel as part of normal business operations, including (for example) name, position title, work telephone number and work email address. This does not extend to the disclosure of private or sensitive personal information of Personnel.

5.5. Law enforcement functions

5.5.1. Council recognises that for several of its functions, including (for example) local laws enforcement, animal management and parking enforcement, it may be classified as a law enforcement agency under Schedule 5 of the IP Act.

5.5.2. Where Council is performing law enforcement functions, certain QPPs may not apply to the extent that Council is satisfied on reasonable grounds that non-compliance is necessary for the performance of those law enforcement functions. Under section 29 of the IP Act, the QPPs that may be disapplied are QPP 3, QPP 5, QPP 6, and QPP 10.

5.5.3. Where Council relies on this exemption, it must document the basis on which it is satisfied that non-compliance is necessary and must limit the departure from the QPPs to what is reasonably required for the law enforcement purpose.

5.6. How Council stores and protects information

5.6.1. Council stores personal information in electronic records management systems, financial systems, human resource systems, and in physical files. Council takes reasonable steps to protect personal information from misuse, interference, loss and from unauthorised access, modification or disclosure, including through:

a) Technical controls, as set out in the ICT Information Security Administrative Policy.

b) Access controls, as set out in the ICT User Access Management Strategic and Administrative Policies.

c) Physical security measures for paper-based records.

d) Contractual obligations on Contracted Service Providers to comply with the QPPs.

e) Training and awareness programs for Personnel, as set out in the ICT Security Awareness Administrative Policy.

5.6.2. When personal information is no longer needed for any purpose for which it may be used or disclosed, Council will take reasonable steps to destroy or de-identify the information, subject to the requirements of the Public Records Act 2023 (Qld).

5.7. Overseas disclosure of personal information

5.7.1. Council does not routinely disclose personal information to entities located outside Australia. However, in limited circumstances, personal information may be transferred or accessible overseas, including where:

a) Council uses cloud-based services, software platforms or data storage hosted outside Australia.

b) Council engages international service providers for specific functions or projects.

c) Disclosure is required or authorised by law, or is made with the individual's consent.

5.7.2. Where Council discloses personal information to an overseas recipient, Council must comply with section 33 of the IP Act. Before disclosing personal information overseas, Council must take reasonable steps to ensure that the overseas recipient does not breach the QPPs in relation to the information.

5.7.3. Where Council is likely to disclose personal information to entities outside Australia, Council will, where practicable, identify the countries in which those recipients are located and publish this information on its privacy webpage.

5.7.4. Council will maintain a record of any overseas disclosures of personal information, including the recipient, the country, the information disclosed, and the basis for the disclosure.

5.8. Data breach

5.8.1. From 1 July 2026, Council is subject to the MNDB scheme under Chapter 3A of the IP Act. Council's response to data breaches, including Eligible Data Breaches, is set out in the Data Breach Statutory Policy.

5.8.2. Personnel must immediately report any actual or suspected data breach in accordance with the Data Breach Statutory Policy.

5.8.3. This policy should be read in conjunction with the Data Breach Statutory Policy.

5.9. Privacy complaints

5.9.1. An individual who believes Council has not complied with the QPPs may make a privacy complaint to Council.

5.9.2. Privacy complaints should be directed to the Responsible Manager in the first instance. Council will:

a) Acknowledge the complaint in writing within ten (10) business days of receipt.

b) Investigate and provide a substantive response to the complaint within forty-five (45) business days of receipt.

c) Where it is not possible to respond within forty-five (45) business days, seek the complainant's agreement to an extension of time and provide written reasons for the extension.

5.9.3. If the individual is not satisfied with Council's response, they may make a complaint to the OIC. The OIC may mediate the complaint or, in certain circumstances, investigate and decide.

5.9.4. Council will manage privacy complaints in accordance with its Complaint Management Policy, ensuring consistency, fairness and procedural integrity. Council will maintain a record of all privacy complaints received and the outcomes, to support continuous improvement.

5.10. Access and amendment

5.10.1. Individuals have the right to request access to personal information Council holds about them and to request amendment of that information where it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

5.10.2. Applications for access and amendment are made under the Right to Information Act 2009 (Qld) and should be directed to Council's RTI Officer. No application fee is payable for access applications limited to documents containing the applicant's personal information, or for amendment applications.

5.10.3. Further details on the access and amendment process are set out in the Right to Information Statutory Policy.

6. Record keeping

6.1. All records relating to actions taken under this policy must be managed in accordance with the Public Records Act 2023 (Qld) and Council's records management requirements.

6.2. A single repository of information must be maintained to document each matter and the response, including all key decision-making records.

7. Training and Awareness

7.1. All Personnel must receive training on their privacy obligations under this policy and the QPPs as part of induction, and at least annually thereafter.

7.2. Training must include what constitutes personal information; how to collect, use and disclose personal information lawfully; the obligation to report data breaches; and how to handle privacy complaints and access requests.

8. Human Rights Consideration

8.1. Council is a public entity under the Human Rights Act 2019 (Qld) and must act and make decisions in a way that is compatible with human rights.

8.2. This policy has been assessed for compatibility with the human rights protected under the Human Rights Act 2019 (Qld). To the extent that this policy may limit human rights, those limitations are considered reasonable and demonstrably justifiable in accordance with section 13 of the Human Rights Act 2019 (Qld).

8.3. This policy engages the right to privacy (section 25 of the Human Rights Act 2019 (Qld)). The policy supports and promotes this right by establishing Council's obligations and procedures for the lawful management of personal information. This policy does not limit any human rights protected under the Human Rights Act 2019 (Qld).

9. Breaches

9.1. Failure to comply with this policy may result in disciplinary action and may also result in decisions being reviewed, suspended, or set aside where required to address risk, probity, or legal compliance.

9.2. Suspected misconduct, fraud, improper influence, or serious probity concerns must be reported in accordance with Council's relevant reporting processes and Code of Conduct.

10. Policy Review

10.1. The policy is to be reviewed in accordance with the Policy Framework.

10.2. Kowanyama Aboriginal Shire Council reserves the right to vary, replace, or terminate this policy from time to time.

11. Approval

11.1. This policy was duly authorised by Kowanyama Aboriginal Shire Council on 26 May 2026 as Kowanyama Aboriginal Shire Council's Information Privacy Policy and shall hereby supersede any previous policies of the same intent.