INFORMATION PRIVACY POLICY

INTENT

This policy establishes Cook Shire Council's framework for the responsible collection, use, storage, and disclosure of personal information. It ensures Council meets its legislative obligations under Queensland's *Information Privacy Act 2009* and the Queensland Privacy Principles while delivering effective services to our community.

SCOPE

This policy applies to all Councillors, Council staff, volunteers, contractors, consultants, and other agents acting on behalf of Council. It covers all personal information collected, used, and stored by Council across every aspect of our operations and service delivery.

POLICY STATEMENT

Privacy Obligations

Cook Shire Council is committed to protecting personal information and maintaining community trust. We understand that safeguarding the privacy of community members, employees, and service users is fundamental to delivering effective local government services.

Personal information is collected only when it is directly relevant and necessary for Council to fulfil its functions, provide services, or meet legal requirements. We do not collect information simply because it might be useful – it must serve a specific, legitimate purpose.

Council complies with the Queensland Privacy Principles under the *Information Privacy Act 2009*. These include:

- Collection principles – ensuring information is collected lawfully, fairly, and only when necessary
- Storage and security – protecting information through appropriate security measures

- Access and transparency – providing individuals with information about documents containing their personal information
- Use and disclosure limits – using information only for relevant purposes and limiting disclosure to authorised parties
- Accuracy requirements – ensuring information is accurate before use and allowing individuals to seek amendments

Collection of Personal Information

Council collects personal information only in the following circumstances:

- With consent – the individual has agreed to provide the information
- To fulfil legal obligations – required under the *Local Government Act 2009* or other legislation that governs our operations
- To deliver services – necessary to provide the specific service or facility that has been requested
- For public safety – to prevent or reduce serious threats to life, health, safety, or welfare of individual or the community
- For legal proceedings – necessary for establishing, exercising , or defending legal claims involving Council

The types of personal information Council may be required to collect and hold includes (but is not limited to):

Contact and Identity Information

- Names and addresses
- Telephone numbers
- Email addresses
- Age and/or date of birth

Property and Services

- Property ownership and /or occupier details
- Library and/or gym membership details
- Animal ownership and registration information

Financial Information

- Payment history and billing records
- Financial information for contractors and service providers
- Pensioner and concession eligibility details

Health Information

- Health information for pensioner unit applicants and residents
- Staff health and safety information
- Health declarations for gym membership and facility use

Council employs robust security measure to safeguard personal information against loss, unauthorised access, modification, disclosure, and misuse. Information is stored in secure Council databases with password protection, access controls, and regular backup procedures to prevent data loss. Council's Information Security Policy provides comprehensive details on these protective measures.

Collection Notices

Council ensure transparency by providing clear collection notices whenever personal information is gathered. All Council forms include a standard notice explaining the legal authority for collection, how information will be managed, and relevant legislative protections.

Individual Privacy Rights

Community members have important rights regarding their personal information:

Access to Personal Information
Under Queensland privacy legislation, you have the right to:

- Request access to documents containing your personal information
- Seek amendment of your personal information if it is incomplete, inaccurate, outdated, or misleading
- Lodge a complaint if you believe your privacy has been breached
- Receive clear information about why your personal information is being collected and how it will be used

Personal details can be updated using forms available on Council's website or by contacting Council to obtain the appropriate form. To access personal information held by Council, individuals can submit an Information Privacy application. Forms and detailed guidance are available on Council's website.

Privacy complaints must be made in writing and can be submitted to Council by:

Email: mail@cook.qld.gov.au

Post: PO Box 3, Cooktown, 4895

Complaints should include the complainant's contact details and specific particulars of the alleged privacy breach or concern. Council will process privacy complaints in accordance with Chapter 5 of the *Information Privacy Act 2009* and Council's complaints management processes.

Privacy Officer

Cook Shire Council's Privacy Officer is the Governance Coordinator, who is responsible for:

- Processing privacy complaints and access request
- Coordinating responses to data breaches
- Providing guidance on privacy matters
- Ensuring compliance with privacy legislation

Access to Council Information

Cook Shire Council operates with a commitment to openness and accountability. Under the *Right to Information Act 2009* (RTI Act), community members can access information about Council's operations, decisions, and activities.

RTI applications are assessed in accordance with legislative requirements and released to applicants unless disclosure would, on balance, be contrary to the public interest. Information may be exempt from release if it contains personal information about individuals other than the applicant, commercially sensitive information, or information that could prejudice Council's functions or operations.

Required Disclosure of Information

There are circumstances where Council is legislatively required to disclose information which may contain personal information. If another law requires personal information to be dealt with in a certain way, Council has not breached its privacy obligations to individuals.

Common situations requiring disclosure:

- Open Council Meetings – Council meetings must be open to the public under local government legislation, making agenda information publicly available. While we exclude personal information where possible, some circumstances require disclosure as part of Council decision making processes.
- Emergency Response – During disasters or emergency situations, we may share personal information with emergency service agencies, Queensland Police, or other authorities to protect life, safety, and property. This enables coordinated response efforts when communities face significant threats.
- Planning and Development – The *Planning Act 2016* requires Council to publish the names of development applicants and submitters at specified stages of the

development assessment process. This transparency supports community participation in planning decisions that affect local areas.

- Other Legislative Requirements – Various laws may require disclosure for purposes such as court proceedings, regulatory compliance, debt recovery, or fulfilling reporting obligations to state and federal government agencies.

In all cases, we limit disclosure to what is specifically required by legislation and take steps to protect sensitive information wherever possible.

Overseas Disclosure Restriction

Council does not disclose personal information to entities outside Australia. All disclosures, whether required by law or otherwise authorised, are limited to Australian-based organisations and government agencies.

Mandatory Notification of Data Breaches

From July 2026, Council will be subject to Queensland's Mandatory Notification of Data Breach (MNDB) scheme under the *Information Privacy Act 2009*. This scheme requires Council to take prescribed actions when responding to data breaches, particularly those classified as 'Eligible Data Breaches'.

What is a Data Breach?

A data breach occurs when there is:

- Unauthorised access to or disclosure of information held by Council, or
- Loss of personal or non-personal information held by Council where unauthorised access or disclosure is likely to occur.

Data breaches can result from various causes including malicious external attacks, human error, or failures in information handling or security systems.

What is an Eligible Data Breach?

An Eligible Data Breach is a data breach involving personal information that is likely to result in serious harm to one or more individuals. This includes situations where there has been:

- Unauthorised access to or disclosure of personal information held by Council, and the access or disclosure is likely to result in serious harm to affected individuals, or
- Loss of personal information held by Council that is likely to result in unauthorised access or disclosure, and the loss is likely to result in serious harm to affected individuals.

Council's Response Obligations

When a data breach occurs, Council must:

Immediate Response

- Contain and mitigate the breach by taking all reasonable steps to limit further unauthorised access or disclosure.
- Assess the situation to determine the scope and potential impact of the breach.

Assessment Requirements

- If Council is uncertain whether a breach constitutes an Eligible Data Breach, we must assess within 30 days whether there are reasonable grounds to believe it is an Eligible Data Breach.
- This assessment period may be extended under specific circumstances as permitted by the Act.

Notification Obligations

To the Office of the Information Commissioner:

- Council must notify the OIC in writing as soon as practicable after determining that a breach is an Eligible Data Breach.
- The notification must include prescribed information about the nature, cause, and impact of the breach.

To Affected Individuals:

- Council must notify individuals whose personal information was involved in an Eligible Data Breach as soon as practicable.
- Notification methods will depend on the circumstances and may include:
    - Direct notification to each individual (by phone, email, letter, or in person) where reasonably practicable.
    - Targeted notification to affected individuals likely to suffer serious harm.
    - Public notification on Council's website for at least 12 months if direct contact is not reasonably practicable.

Information to be Provided

Notifications to affected individuals must include (where reasonably practicable):

- The date the breach occurred
- A description of the breach and how it occurred

- The personal information involved in the breach
- The duration of any unauthorised disclosure
- Actions taken or planned to secure the information and mitigate harm
- Recommended steps individuals should take in response
- Information about complaint and review processes
- Contact details for further inquiries

Factors for Assessing Serious Harm

When determining whether a breach may result in serious harm, Council will consider:

- The kind and sensitivity of personal information involved
- Whether the information was protected by security measures and the likelihood these could be overcome
- Who has or could obtain the personal information
- The nature of harm likely to result from the breach
- The number of individuals affected
- How easily individuals can be identified from the information
- Any existing mitigating measures

Exemptions

Notification may not be required in certain circumstances, such as when:

- The breach is unlikely to result in serious harm
- Remedial action has been taken that significantly reduces the risk of serious harm
- It would be unreasonable in the circumstances to require notification

Record Keeping

Council will maintain:

- A Register of Eligible Data Breaches documenting all breaches that meet the threshold for notification
- Comprehensive records of all data breach incidents, assessments, and responses
- Documentation of decision-making processes and actions taken

Roles and Responsibilities

All Council staff must:

- Immediately report suspected data breaches to their supervisor or the Privacy Officer

- Cooperate with breach response activities
- Comply with security measures and protocols

Privacy Officer will:

- Assess the severity of data breaches and likelihood of serious harm
- Coordinate notifications to the OIC and affected individuals
- Maintain the Register of Eligible Data Breaches
- Escalate serious breaches to senior management

Senior Management will:

- Oversee the breach response process for significant incidents
- Make final decisions on notification requirements
- Ensure adequate resources are allocated to breach response
- Review and improve data breach policies and procedures

Continuous Improvement

Following any data breach, Council will:

- Conduct a post-incident review to identify lessons learned
- Implement remediation measures to prevent similar breaches
- Update security measures, policies, and procedures as necessary
- Provide additional staff training where required

This framework ensures Council meets its legal obligations while maintaining transparency and accountability to our community in protecting their personal information.

KEY RESPONSIBILITIES

RESPONSIBLE OFFICER	RESPONSIBILITY
All Council Staff	• Treat all personal information with care and respect, recognising that protecting community privacy is a shared responsibility. • Only collect, access, use, and disclose personal information that is necessary for legitimate Council business purposes. • Follow the "need to know" principle – only access information required to perform assigned duties and responsibilities.

RESPONSIBLE OFFICER	RESPONSIBILITY
	• Store personal or sensitive information securely, whether in physical or electronic form, and never leave it unattended or accessible to unauthorised persons. • Use Council-approved systems and methods for transmitting personal information, avoiding unsecured email or messaging platforms. • Immediately report any suspected data breach, privacy incident, or unauthorised access to personal information to a supervisor, manager, or Privacy Officer. • Be alert to potential privacy risks in daily work practices and proactively seek guidance when uncertain about information handling requirements. • Complete mandatory privacy training and stay current with Council's privacy policies and procedures. • Maintain confidentiality of personal information both during employment and after leaving Council.
Records Management Officers	• Ensure personal information is classified, stored, and managed in accordance with approved retention and disposal schedules. • Implement and maintain management systems that support privacy compliance and secure information handling. • Ensure records containing personal information are appropriately protected and accessible for privacy requests. • Develop and deliver training on secure records handling practices for all Council staff. • Monitor compliance with information handling procedures and report potential privacy risks to appropriate officers.
ICT Officer	• Design, implement, and maintain technical safeguards to protect personal information from unauthorised access, disclosure, or loss. • Monitor information systems for security vulnerabilities and potential data breaches, and implement response protocols. • Ensure backup and recovery systems are in place to restore personal information following system failures or security incidents.
Executive Leadership Team	• Provide leadership and commitment to privacy protection as a core organisational value.

RESPONSIBLE OFFICER	RESPONSIBILITY
	• Ensure adequate resources are allocated for privacy compliance, including staffing, training, and technology investments. • Make final decisions on significant privacy matters, including major data breach responses and policy changes.
Governance Coordinator	• Coordinate the development, review, and update of privacy-related policies and procedures across Council. • Process and respond to privacy complaints, access requests, and amendment applications from community members. • Provide clear communication to individuals about their privacy rights and how to exercise them. • Serves as designated Privacy Officer; oversees privacy governance and compliance.

DEFINITIONS

TERM	DEFINITION
Agency	Cook Shire Council or any entity subject to the *Information Privacy Act 2009.*
Collection	Gathering, acquiring or obtaining personal information from any source and by any means, including information that Council has obtained accidently or has not specifically requested.
Council	Cook Shire Council.
Data Breach	The unauthorised access to, or unauthorised disclosure of, information held by Council, or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
Disclosure	The release of personal information to persons or organisations outside of Council. It does not include providing individuals with access to their own personal information.
Eligible Data Breach	A data breach involving personal information that is likely to result in serious harm to any individual to whom the information relates. This includes situations where there has been: • Unauthorised access to our disclosure of personal information held by Council, where the access or

TERM	DEFINITION
	disclosure is likely to result in serious harm to affected individuals, or • Loss of personal information held by Council that is likely to result in unauthorised access or disclosure, where the loss is likely to result in serious harm to affected individuals.
IP Act	The *Information Privacy Act 2009* (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.
Privacy Officer	The Council officer designated with responsibility for privacy matters, including assessment of data breaches, coordination of notifications, and maintenance of privacy compliance.
Public Interest	Considerations that favour disclosure of information to the community, balanced against factors that favour non-disclosure, as assessed under the *Right to Information Act 2009.*
Queensland Privacy Principles (QPPs)	The thirteen (13) privacy principles set out in the *Information Privacy Act 2009* that govern how public sector agencies must handle personal information, covering collection, storage, security, access, use, and disclosure.
Register of Eligible Data Breaches	The record maintained by Council documenting all data breaches that meet the threshold for mandatory notification under the IP Act.
RTI Act	The *Right to Information Act 2009* (Queensland).
Serious Harm	In relation to an individual and unauthorised access to or disclosure of, the individual's personal information, includes serious physical, psychological, emotional, financial harm, or serious harm to the individual's reputation.
Suspected Eligible Data Breach	A data breach where Council has reasonable grounds to suspect it may be an Eligible Data Breach but requires further assessment to determine whether it meets the threshold for mandatory notification.
Unauthorised Access	Access to personal information by a person who is not permitted to access that information, or access that exceeds the level of access a person is permitted to have.

TERM	DEFINITION
Unauthorised Disclosure	The release, publication, or making available personal information, or access that exceeds the level of access a person is permitted to have.

REFERENCES, LEGISLATION AND GUIDELINES

Information Privacy Act 2009 (Qld)
Right to Information Act 2009 (Qld)
Local Government Act 2009 (Qld)
Public Records Act 2023 (Qld)
Planning Act 2016 (Qld)

RELATED DOCUMENTS

Information Security Policy
Confidential Information Policy
Closed Circuit Television (CCTV) Policy
Administrative Action Complaint Management Policy
Administrative Instruction – Records Management
Data Breach Response Plan (under development)

IMPLEMENTATION/COMMUNICATION

Upon adoption, this policy will be distributed to all staff and integrated into organisational operations. Policy requirements will be communicated to new staff through induction programs and reinforced through ongoing training and awareness initiatives.

APPROVED BY

Council Resolution 2025/170

REVIEW

SPONSOR:	Manager of the Office of the CEO
OFFICER RESPONSIBLE FOR REVIEW:	Governance Coordinator
ADOPTION DATE:	26 August 2025
REVIEW DATE:	August 2028

THIS POLICY IS TO REMAIN IN FORCE UNTIL OTHERWISE DETERMINED BY COUNCIL

AMENDMENT HISTORY

VERSION	AMENDMENT DETAILS	AMENDMENT DATE	APPROVAL
1.0	New policy	26 August 2025	Council resolution 2025/170