Information Privacy		
	Approved by CEO:	
		16 July 2025
	Considered by ELT:	30 June 2025

Policy purpose

The purpose of this policy details how Sunshine Coast Council (Council) will manage and protect the personal information of individuals in accordance with the *Information Privacy Act 2009* (the **IP Act**) and its Queensland Privacy Principles (QPPs).

Policy scope

The policy applies to all the following:

- The Mayor, Councillors, Chief Executive Officer (CEO), Directors, Managers, employees, contractors, work experience students, apprentices, volunteers, consultants, contingent workers, vendors, contracted external service providers and outsourced business functions who handle personal information on behalf of Council.
- All personal information, collected, stored, used, and disclosed by Council, regardless of format, medium and source, unless otherwise exempted by legislation.
- All administrative and technological environments in which Council's business is conducted.
- Information systems regardless of whether manual or automated.

Policy statement

Council recognises that privacy is a human right. Council is committed to protecting and respecting the privacy of all individuals.

The IP Act places obligations on Council, including the need to comply with:

- the Queensland Privacy Principles;
- conditions under which personal information may be transferred outside of Australia;
- rules regarding contracted service providers; and
- the right for individuals to access and amend their personal information.

Further to this, the right to privacy and reputation is included in the *Human Rights Act 2019*. Council recognises and is committed to act compatibly with these rights.

This policy is further supported by guidelines which must be complied with in accordance with this policy.

Principles

The principles that guide the application of this policy are:

Council will-

- collect, use, disclose, amend, provide access, store, purge and secure personal information in accordance with the IP Act and the QPPs, which are summarised in Appendix 2.
- demonstrate transparency about how Council handles personal information, including by:
    - publishing clear, helpful, accurate and up-to-date information which makes it easy for people to understand any collection, use and disclosure and the associated purposes
    - ensuring that people are notified and informed at any time when personal information is collected, including through appropriate privacy notices on Council forms and signage where videos or photographs may be captured.
- educate and inform employees about protecting personal information under the *Information Privacy Act 2009* and the right to privacy and reputation under the *Human Rights Act 2019*.
- apply the QPPs as an integral part of its business processes
- ensure privacy impact assessments are considered as an integral part of the planning and risk management processes for information management systems and information collection
- ensure all privacy breaches and complaints are contained, assessed, notified, and reviewed in accordance with the IP Act
- ensure any personal information transferred outside of Australia is in accordance with IP Act s33.
- ensure all contracted service providers are bound by the requirements for handling of personal information as per chapter 2, part 3 of the IP Act

Policy application

Transparent handling of personal information

To demonstrate transparent handling of personal information and ensure compliance with QPP 1, Council will maintain a dedicated webpage to cover the following:

- the kinds of personal information Council collects and holds
- how Council collects personal information and sensitive information
- the purposes for which Council collects, holds, uses and discloses personal information
- how people may access their personal information held by Council
- dealing with customers who wish to remain anonymous or use a pseudonym
- security of personal information
- how to make a privacy complaint and how Council will handle such complaints
- details of any likely disclosures outside of Australia

All branches or areas within the organisation which handle personal information will assist with keeping this webpage updated and accurate, and to help ensure that it captures all of Council's different functions and activities which involve the management or handling of personal information. All forms, signage and similar disclaimers to warn and inform people about collection of their personal information must contain a link to the webpage.

Ensuring officers are informed and empowered

Council officers who handle or access personal information are empowered to ensure that personal information is protected and respected, including to raise concerns and address potential risks.

Officers must have good awareness of relevant privacy risks and restrictions that apply to their ordinary work and responsibilities. All Council officers will receive regular training about the requirements of privacy legislation and this policy.

Policy review

This policy will be reviewed in accordance with Council's Policy Framework and will be reviewed at least every four years.

Roles and responsibilities

Role	Responsibility
Council	Maintains awareness of organisational policies. Provides feedback to the CEO when consulted (on policies which apply to Councillors or where this policy impacts the community).
Chief Executive Officer (CEO)	Approval authority for setting this policy and for all material changes to this policy, on advice from ELT. Able to approve non-material changes. CEO will consult with Councillors where this policy applies to Councillors or impacts the community.
Executive Leadership Team (ELT)	Provides advice to the CEO on setting this policy and all proposed material changes to this policy. Provides feedback to the policy sponsor and policy holder regarding the scope of approaching reviews.
Director, Business Transformation and Performance	Policy sponsor. Approval authority for any non-material change to this policy.
Manager, Ethical Standards	Policy holder. Approval authority for any minor non-material changes to this policy.
Coordinator, Integrity Management	Leads this policy's development, including communication, implementation, review and reporting.

Measurements of success

The success of this policy will be measured by:

Measure	Outcome sought
Designated officers across the organisation are given responsibility to regularly review Council's privacy webpage and initiate updates	Council's privacy webpage is kept updated with open, transparent and accurate information to cover all of Council's activities which involve the management of personal information
Designated officer approves all privacy impact assessments	Privacy impact assessments are conducted as part of the planning and risk management processes for information management systems and information collection
All officers receive training annually about their role and responsibilities for handling and accessing personal information	Officers are empowered to avoid, identify and mitigate privacy risks, including common risks that may arise as part of their everyday work

Definitions

Refer to Council's Policy Framework for definitions of common terms. The following contains definitions for terms specific to this policy. For otherwise undefined terms, the plain English meaning informs interpretation.

Term	Definition
Disclosure	Refer to section 23 of *the Information Privacy Act 2009*
Queensland Privacy Principles or QPPs	Schedule 3 of the *Information Privacy Act 2009* contains the Queensland Privacy Principles (QPPs) which set out the rules for how Queensland Government agencies handle personal information. A summary is provided in Appendix 2.
Personal information	Personal information means 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. Personal information is inclusive of Sensitive Information.
Sensitive information	Sensitive information is information or an opinion about an individual's: • racial or ethnic origin • political opinions

	• membership of a political association • religious beliefs or affiliations • philosophical beliefs • membership of a professional or trade association • membership of a trade union • sexual orientation or practices • criminal record • health information • genetic information that is not otherwise health information • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.

Appendix 1

Policy information		
Title	Information Privacy	
Purpose	The purpose of this policy details how Sunshine Coast Council (Council) will manage and protect the personal information of individuals in accordance with the *Information Privacy Act 2009* (the **IP Act**) and its Queensland Privacy Principles (**QPPs**).	
Document number	EDDIE Ref: D2023/333887	
Corporate Plan reference	**Goal** **Pathway** **Service Output**	Organisational Excellence Build Community Trust Governance
Category	Governance	
Subcategory		
ELT advice date	30 June 2025	
CEO approval date	16 July 2025	
Effective date	16 July 2025	
Review schedule	A full review must be undertaken within every four years, and reviewed policy document must be provided to highest level approval authority for endorsement. Reviews may occur more regularly as required, having regard to a policy risk assessment.	
Last review	2021	
Next review	2029	
Policy holder	The Manager responsible for this policy is: Manager, Ethical Standards Branch	
Approval authority	CEO has authority to endorse material changes on advice of ELT. Relevant Director has authority to approve non-material changes. Relevant policy holder has authority to approve minor non-material changes.	

Sunshine Coast COUNCIL

Related documents	
Legislation	*Information Privacy Act 2009* *Right to Information Act 2009* *Human Rights Act 2019* *Local Government Act 2009* *Public Records Act 2023* *Spam Act 2003* (Cth) *Invasion of Privacy Act 1971*
Policy	Administrative Access and Right to Information Policy SCC Employee Code of Conduct SCC Information Access and Management Policy SCC Records Management Policy
Operational documents	

Version Control

Version	Reason/Trigger	Change	Endorsed/Reviewed by	Date
1.0	Scheduled Review. Human Rights Compatibility assessed.	Updated to reflect amendments to IP Act.	ELT CEO	30/6/2025 16/07/2025

Sunshine Coast COUNCIL

Appendix 2 - Summary of the Queensland Privacy Principles

QPP 1 — Open and transparent management of personal information

Requires agencies to manage personal information in an open and transparent way.

Requires a clear, up-to-date and accessible QPP privacy policy, and practices and procedures to ensure QPP compliance.

QPP 2 — Anonymity and pseudonymity

Requires agencies to allow individuals the option of not identifying themselves (i.e. to deal with the agency anonymously or pseudonymously) unless it is:

- required or authorised under law, or
- impracticable.

QPP 3 — Collection of solicited personal information

Provides that agencies:

- can only collect personal information that is reasonably necessary for, or directly related to, one of their functions or activities
- must collect it lawfully and fairly, and
- must collect it from the individual unless an exemption applies (including consent, lawful authority/requirement and law enforcement),or it is unreasonable or impracticable to do so.

Higer standards apply to the collection of sensitive information.

Personal information is only *collected* if the agency solicits it, i.e., they ask someone for it or otherwise takes active steps to acquire it. Unsolicited personal information sent to an agency is not collected and must be assessed under QPP 4.

QPP 4 — Dealing with unsolicited personal information

Requires agencies to assess *unsolicited* personal information to determine whether they could have collected it under QPP 3 and/or whether it is a public record. If not, agencies may be required to destroy or de-identify unsolicited personal information, subject to public record laws. Otherwise, QPPs 5 to 13 apply.

QPP 5 — Notification of the collection of personal information

Requires agencies that collect personal information to take reasonable steps to make sure individuals are aware of the matters listed in QPP 5 including agency contact details, the fact and circumstances of the collection if collected from someone other than the individual and the consequences if the information is not collected.

This applies when personal information is collected from an individual or from a third party.

Agencies do not need to provide a formal QPP 5 notice. The QPP 5 matters can be communicated in other ways, for example, informally or verbally.

QPP 6 — Use or disclosure of personal information

Agencies can only use or disclose personal information for the reason it was collected, unless QPP 6 allows it to be used or disclosed for a secondary purpose. These include:

- instances where the individual has consented to the use of disclosure of the information
- QPP 6 specific secondary purposes, including where:
  - the individual would reasonably expect the agency to use or disclose the information for the secondary purpose (subject to limitations)
  - where it is required or authorised by law or reasonably necessary for law enforcement activities
- permitted general situations such as lessening or preventing a serious threat or locating a missing person (set out in schedule 4, part 1 of the IP Act), and permitted health situations (set out in schedule 4, part 2 of the IP Act).

QPP 10 — Quality of personal information

Requires agencies to take reasonable steps to ensure the personal information:

- they collect, use, or disclose is accurate, up to date, complete, and
- for use or disclosure, is relevant to the purpose of the use or disclosure.

QPP 11 — Security of personal information

Requires agencies to *take reasonable steps to protect* the personal information it holds from

- misuse, interference or loss, and
- unauthorised access, modification or disclosure.

Requires agencies to take reasonable steps to destroy or deidentify personal information that is no longer needed for any purpose and is not a public record or otherwise required to be retained under law or court or tribunal order.

QPP 12, QPP 13 — Access to/correction of personal information

Requires agencies to give access to and correct personal information they hold, subject to limitations.

The following QPP's are not used (i.e. the corresponding Australian Privacy Principles (APPs) were not implemented in the IP Act):

- QPP 7 – Direct marketing
- QPP 8 — Cross-border disclosure of personal information, noting that similar requirements to APP 8 are contained in s.33 of the IP Act
- QPP 9 — Adoption, use or disclosure of government related identifiers.

Sunshine Coast COUNCIL