

1. Purpose

The purpose of this policy is to outline Council's commitment to maintaining a culture that respects each individual's right to privacy and sets out Council's position and principles in relation to the management of personal information as required by the *Information Privacy Act 2009* (IP Act), *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA) and the management of confidential information as required by the *Local Government Act 2009* (the Act). The IP Act and IPOLA establish the standard for how Queensland government agencies handle personal information through the Queensland Privacy Principles (QPP), including the requirement, under QPP 1, that every agency must have a QPP privacy policy.

Council's Privacy Policy incorporates the Queensland Privacy Principles (QPP's) and explains how personal information is managed, including:

- (a) the kinds of personal information we collect and hold, how we collect and hold that personal information, and the purposes for which we collect, hold, use and disclose personal information; and
- (b) how complaints can be lodged regarding Council handling a person's personal information, and how we will deal with the complaint.

2. Scope

This policy applies to all Councillors, employees and contractors working for Council regardless of whether they are permanent, temporary, full-time, part-time or casual and to the personal information we collect, store, manage, use and disclose in discharging most of our statutory functions and delivering services to the community. For the purposes of this policy, the term contractor includes temporary labour services (agency staff) and sub-contractors.

This policy applies to all personal information handled by Council in the course of performing its legislative, administrative and operational functions. It covers personal information in any format, including paper records, electronic data, emails, photographs, CCTV footage, audio or video recordings, and information stored or processed through approved third-party or cloud-based systems.

3. Responsibility

The Chief Executive Officer (CEO) is the principal officer of Council and is responsible for ensuring Council's administrative procedures and management of information practices adhere to privacy obligations under the IP Act and IPOLA.

The Director Corporate, Community and Development Services (DCCDS) is responsible for ensuring and managing privacy compliance, reporting and providing advice to members of the public and employees about Council's privacy obligations. This includes:

- Ensuring employees have access to adequate training materials in relation to privacy compliance;
- Having delegated authority to:
 - Investigate and make decisions about all privacy complaints and breaches of privacy; and
 - Coordinate information privacy requests and information privacy amendment requests.
- Assisting directorates and teams in conducting privacy impact assessments (PIA's) when designing and implementing new projects and programs that involve the management of personal information; and

- Maintaining and periodically reviewing this policy and any associated procedures.

Directors, Managers and Supervisors are responsible for:

- Ensuring their directorates and teams comply with all policies and procedures in place to maintain and uphold confidentiality, the Queensland Privacy Principles (QPPs), the IP Act and IPOLA;
- Ensuring employees are educated about their privacy compliance obligations;
- Referring all complaints and breaches to the DCCDS; and
- Seeking advice from the DCCDS when considering new projects or programs that involve the management, use or disclosure of personal information.

The Senior Records Officer (SRO) is the officer delegated as the Privacy Officer to handle any information privacy complaints, enquiries and requests under the guidance of the Business Services Coordinator and Director Corporate, Community and Development Services.

All Councillor's and Council employees must:

- Ensure that the personal and confidential information they handle is managed in accordance with the QPPs, the IP Act, IPOLA, this policy and supporting procedure/s;
- Exercise due care when handling or using information acquired in their role with Council and if uncertain, presume that information is confidential, and seek advice from the DCCDS prior to releasing it;
- Report all suspected or actual breaches of privacy to the Privacy Officer, Business Services Coordinator or the DCCDS for investigation and decision; and
- Not access or attempt to access personal or confidential information that is not required for their role.

Council is committed to ensuring that privacy obligations are embedded across all functions, systems and work practices. Each directorate is responsible for integrating privacy considerations into its planning, decision-making and service delivery activities, and for ensuring that any new or amended processes, technologies or programs involving personal information are assessed for privacy impacts and managed in accordance with the Queensland Privacy Principles and relevant legislation.

4. Definitions

The following definitions apply to this Policy and to the Information Privacy Management Procedure.

Anonymity means that an individual can interact with Council without identifying themselves. Council must offer anonymity where lawful and practicable, in accordance with QPP 2.

Confidential information is information generally not known by, or available upon request to, the public which:

- Identifies and relates to a particular individual; or
- Carries a risk that – if released or improperly used – would cause harm to the council or a member of the community, or give an unfair advantage to someone.

Councillor means all elected representatives, including the Mayor.

Data Breach occurs when personal information is lost, accessed, used, modified or disclosed without authorisation, or is otherwise compromised.

Disclosure means making personal information available outside of Council, including to another agency, organisation, contractor or individual, whether intentionally or unintentionally.

Employee is any person employed directly by Hinchinbrook Shire Council regardless of their employment status, and contractors undertaking duties on behalf of Council.



Queensland Privacy Principles (QPPs) as contained in the *Information Privacy Act 2009* (Schedule 3).

Personal information as defined in the *Information Privacy Act 2009*:

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 any information that may lead to the identity of a person. For information to be personal information, two criteria must be satisfied:

- It must be about a living individual; and
- The individual's identity must be apparent or reasonably ascertainable from the information.

There are some obvious examples of personal information such as a person's name and address, but it can also include information about a person's health, criminal or financial records and email addresses.

Information does not have to be true in order to be personal information and it does not need to be written down or recorded in another material form, such as a photograph or audio.

Routine personal work information relates solely to the work duties of a public-sector employee and is found in almost all documents held by Council.

When disclosing routine personal work information for a legitimate function of Council, the infringement of a public-sector employee's right to privacy would, generally, be minimal or non-existent as the disclosure would be a matter of expectation in the legitimate course of their employment.

Privacy Breach is any failure by Council to comply with the *Information Privacy Act 2009* or the Queensland Privacy Principles in the handling of personal information.

Pseudonymity means that an individual may use a name, reference number or other identifier that is not their legal identity when interacting with Council, where lawful and practicable.

Public Record is any recorded information created or received by Council in the course of official business, regardless of format, and must be managed in accordance with the Public Records Act 2023.

Reasonably Identifiable - An individual is reasonably identifiable if their identity can be determined from the information alone or in combination with other information that Council holds or can access.

Routine personal work information includes:

- A work email address or work phone number;
- Authorship of a work document, for example, where the person's name is listed as one of the authors of a report;
- A professional opinion given wholly in a professional capacity;
- A position classification, for example, "Planning Officer"; and
- A work responsibility, for example, that the officer is the contact person in response to a complaint or query from a member of the public; information about qualifications held where they are required for the officer's position, for example, where a Senior Engineer holds an engineering degree.

Sensitive Information an individual, means the following:

- (c) information or an opinion about an individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or

- (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual orientation or practices; or
 - (ix) criminal record; or
- (d) health information about an individual; or
- (e) genetic information about an individual that is not otherwise health information; or
- (f) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- (g) biometric templates.

Third Party is any individual or organisation other than the person the information is about, Council staff, or Council's contracted service providers acting on Council's behalf.

Unsolicited Personal Information is personal information received by Council that was not requested or sought. Council must handle such information in accordance with the IP Act and the Public Records Act 2023.

Use refers to the handling of personal information within Council, including accessing, reviewing, analysing or making decisions based on that information.

5. Policy

5.1 Collection of personal and sensitive information

Personal information

Council is committed to protecting the privacy of individuals.

Council collects personal information directly from individuals who access our services and indirectly from third parties as part of carrying out statutory functions and delivering services.

The kind of personal information collected from individuals directly includes names, contact details and details of individuals' interactions with Council. This information may be collected through written correspondence, verbal communication, or electronic submissions, and is gathered only where it is necessary to perform our functions or meet legal obligations.

Council will not disclose your personal information to other government agencies, organisations, or third parties unless:

- You have provided express or implied consent;
- You would reasonably expect us to do so, or we have informed you of the disclosure;
- The disclosure is required or authorised by law;
- It is necessary to prevent or reduce a serious and imminent threat to life, health, or safety;
- The disclosure is reasonably necessary for law enforcement purposes or the protection of public revenue.

Council will take reasonable steps to ensure individuals are aware of the purpose for which their personal information is being collected, the legal authority for the collection, and to whom the information is normally disclosed. Collection will be conducted in a lawful, fair and transparent manner, and only to the extent necessary for Council to perform its statutory responsibilities or deliver services to the community.



Sensitive information

Council may also collect sensitive information. We will generally only collect sensitive information directly from the individual it is about or with their consent, or otherwise consistently with our obligations under the IP Act.

The kinds of personal information and sensitive information we collect and hold, are set out in the following table.

TYPES OF INFORMATION COLLECTED (including sensitive information)	
Term	Kind of personal information, how and why we collect that personal information
Customer Service Requests including Information and Assistance	Council collects and holds personal information about people who contact the Council by phone, in person, post, or email. This information may include names, contact details, and the enquirer's circumstances which led to or are relevant to their enquiry; this can include sensitive personal information, opinions about other people, and expressions of dissatisfaction.
Complaints Management	Council may hold and collect personal information about individuals who make complaints to or against Councillors, Council, services, decisions (or lack of) and actions (or lack of). This may include: names, contact details, details of their complaint and what outcome the individual is seeking. Failure to provide this information may mean that Council is unable to adequately resolve the complaint. As part of conducting reviews or investigations of matters, Council may acquire copies of documents that are relevant to the complaint, which can contain personal information of the individual and related third parties. Council may ask the individual or relevant third parties to provide information in order to resolve the complaint, including their views, opinions and relevant background information. Council may also collect and hold information about reasonable accommodations required by an individual submitting a complaint.
Human Resources	Council collects and holds personal information about Council staff, contractors, volunteers, Councillors and interns/work experience students relevant to their employment or engagement with Council, including contact details, date of birth, tax file number, qualifications, work history, salary and entitlements, and next of kin and/or emergency contacts, as well as information relating to industrial disputes, conflicts of interest, safety investigations, medical information, disciplinary proceedings, equal opportunity data, emergency contact details, workers compensation claims and the names of individuals who are classified as related parties of Councillors and key management personnel.
Recruitment and Engagement of Contractors	Council collects and holds personal information about individuals who apply to work at or with Council. This includes names, contact details, application documents, identification, employment experience, qualifications, assessments for suitability, medical information, referees and references. When engaging contractors, Council uses VendorPanel and also collects and holds information about insurance, subcontractors, commercial in confidence, trade pricing, ABN numbers, details of any statutory notices issued membership of professional or trade associations and other information that may be submitted as part of a tender process.

TYPES OF INFORMATION COLLECTED (including sensitive information)	
Term	Kind of personal information, how and why we collect that personal information
Intergovernmental Communications	Council collects personal information during routine communication exchanges with other local and state government departments. Examples include consultations on development related matters or land valuations resulting from changes in property ownership and citizenship ceremonies.
Information collected via Council's website including online services	Council's corporate website is hosted in Australia. Council's web measurement tools and internet service providers record only anonymous information about site visitors for statistical purposes including: • server and IP address; • name of the top-level domain (e.g. .gov, .com, .edu and .au); • type of browser; • date and time of access; • pages accessed and documents downloaded; and • previous site visited. Council collects personal information through the website where it is provided by individuals who use an online form (e.g. to request a service, register to participate in training or events, lodge a complaint, etc.). Council uses cookies to collect information on website activity (such as number of users, who visits the website, date and time of the visits, number of pages viewed and navigation patterns) for statistical purposes. The information on its own does not identify an individual. Website analytics are captured for the purpose of improving Council's website. Cookies allow computers to identify and interact more effectively and are generated when users log onto or use Council public websites. Users can manage cookies via browser settings giving the user the choice whether to accept or not. Social plug-in tracking cookies may also be used to track both members and non-members of social networks for additional purposes such as behavioural advertising, analytics and market research.
Disaster Response and Recovery	Council uses the Guardian program (provided by QIT Plus) to keep the public informed and to respond during disasters. Information collected includes name, address, contact details, location, disaster information or requests for service or advice.
Surveys and Community Engagement	Council may invite members of the community to undertake community engagement. If an individual agrees to participate in such engagement, Council will collect and hold their personal information using the Council website and Microsoft Forms. In some limited circumstances, Survey Monkey may also be used. Information collected may include name, email, IP address, opinions expressed and responses to matters raised.
Social Media Platforms	Council uses Facebook, LinkedIn and Instagram to communicate with the public about its work and raise awareness of issues affecting the community. When individuals communicate with Council via these social media platforms, Council will collect personal information individuals provide when they communicate with Council.

TYPES OF INFORMATION COLLECTED (including sensitive information)	
Term	Kind of personal information, how and why we collect that personal information
Events, training registrations and Facility bookings	Council collects personal information that individuals provide to Council via Hinchinbrook Tickets or Council's website when registering and/or attending Council events or Facilities and community meetings or participating in events such as the Baby Welcoming Ceremony, Tea and Trivia Morning Tea, Tasman Turtle Picnic Day, Seniors Morning Tea and Christmas in Hinchinbrook for example. This information may include names, contact details, credit card details, bank account, IP address, browser type, device type, vehicle registration number and navigation patterns.
Library	Council uses the Aurora Library Management System to manage library bookings and customer management. This information may include names, address, date of birth, email and phone numbers. The Archives Department stores historical names and information using Enterprise Content Management software.
Water Services	Council invites ratepayers to use the Aqualus H2O portal to monitor their water usage. The information collected includes, name, contact details, address details, property location and water usage.
Audio and Visual Recordings (CCTV)	Council collects audio and visual recordings and live streaming of Council events at various Council facilities and in the community, which includes the images and/or voices of individuals and that may be used to enable the identification of particular individuals. It also collects images and interactions through body worn cameras. Refer to Council's CCTV and Recording Devices Policy for further information.

5.2 Using and Disclosing Personal Information

Council will use and disclose personal information for the purpose for which the personal information was collected, including:

- i. exercising our powers or performing our statutory functions and duties as a regulatory authority and service provider to the community such as assessment and handling of application forms, handling of complaints or responding to general enquiries; and
- ii. Managing associated business functions such as recruitment and human resources administration.

Council may also use or disclose personal information for secondary or alternative purposes as permitted under the IP Act. This may include where Council is authorised or required under Australian law, with the individual's consent, or where the individual QPP Privacy Policy would reasonably expect Council to use or disclose the information for a secondary purpose where it relates to the primary purpose. This includes disclosure to a court or tribunal. Council retains contact details of individuals (including personal information of individuals with whom it does business) in a Customer Relationship Management (CRM) database.

5.3 Holding and Protecting Personal Information

Council is committed to ensuring the security of personal information collected and retained, protecting it from misuse, interference, loss and unauthorised access, modification or disclosure. Council uses physical and electronic security measures including restricting physical access to its offices, ensuring information can only be accessed by authorised staff, firewalls and databases to keep personal information secure.

Where permitted by the *Public Records Act 2023*, Council will destroy or de-identify unsolicited personal information and destroy personal information that is no longer required for the purpose for which it was originally collected in accordance with Council's obligations under the QPPs. If Council suspects or has reason to believe there has been unauthorised access or disclosure of personal information, all necessary actions required by the Mandatory Notifiable Data Breach Scheme will be undertaken once the Scheme legislatively commences.

5.4 Disclosure of Personal Information Outside of Australia

In complying with its obligations under the IP Act, Council will disclose an individual's personal information to someone outside Australia only if:

- the individual agrees to the disclosure;
- the disclosure is authorised or required by law;
- Council is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or
- two or more of the following apply:
 - Council reasonably believes that the recipient is subject to the law, binding scheme or contract that effectively upholds the principles for the fair handling of personal information that are substantially similar to the QPPs.
 - The disclosure is necessary for the performance of Council's functions in relation to the individual.
 - The disclosure is for the benefit of the individual, but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement.
 - Council has taken reasonable steps to ensure the personal information it discloses will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the QPPs. When individuals communicate with Council through social media, survey and event management platforms, the providers and its partners may collect and hold personal information overseas.

Where Council uses digital platforms, cloud-based services or third-party providers that store or process information outside Australia, Council will take reasonable steps to ensure those providers handle personal information in a manner consistent with the Queensland Privacy Principles. Individuals should be aware that by engaging with Council through externally hosted platforms, their personal information may be transferred or stored overseas in accordance with the provider's terms and privacy practices.

5.5 Contracted Service Providers

Council will take all reasonable steps to ensure contracted service providers comply with the requirements of the IP Act when they are provided with or collect personal information in order to provide services on behalf of Council.



Council may require contracted service providers to implement appropriate security controls, report any suspected or actual privacy breaches to Council immediately, and permit Council to review or audit their information-handling practices. Contracted service providers must use personal information only for the purpose of delivering the contracted service and must not disclose, transfer or retain personal information beyond what is authorised by Council.

5.6 Access and Amendment of Personal Information

Individuals may apply for access to, and amendment of, personal information held by Council in accordance with in the RTI Act. An individual has the right to access their personal information held by Council, subject to applicable exemptions, and request the correction of inaccurate or incomplete information.

Requests should be made in writing and include sufficient detail to identify the information. Council will respond in accordance with the timeframes and requirements set out in the *Right to Information Act 2009*. Further information for access and amendment to personal information can be found in the Right to Information procedure.

To access or correct personal information, direct all requests in writing to:

Privacy Officer
Hinchinbrook Shire Council
council@hinchinbrook.qld.gov.au
PO Box 366
INGHAM QLD 4850

Council may require individuals to provide proof of identity before granting access to personal information, and may refuse access where disclosure would unreasonably impact the privacy of another person or where an exemption under the Right to Information Act 2009 applies. Council will take reasonable steps to ensure that any amendments requested are accurate, complete and up to date, and may annotate rather than alter records where appropriate.

5.7 Dealing with Council anonymously or using a pseudonym

A person may interact with Council anonymously or by using a pseudonym.

Requests for service and complaints lodged to Council can be made anonymously or by using a pseudonym. Depending on nature of the request for service or complaint, Council may not be able to further action and/or provide a response without a person's identity (e.g. where a complaint relates to a particular individual's file).

Where a person is lodging a complaint against Council, it is preferred that the individual use their correct full name so that Council can investigate the complaint in full.

Anonymous or pseudonymous interactions is not possible for some functions of Council, such as applying for an internal review or lodging a privacy complaint. Council is required to collect information such as your name, contact details and details of your matter so we can deal with you and your matter effectively and in accordance with our statutory duties.

Council will take reasonable steps to allow individuals to interact anonymously or through a pseudonym where it is lawful and practicable to do so. However, where identity verification is required to fulfil a statutory function, ensure procedural fairness, or protect the rights of other individuals, Council may be unable to provide services or progress a matter without sufficient identifying information.

5.8 Privacy complaints

If you believe that Council has not handled your personal information in accordance with the IP Act, you can make a privacy complaint. You can only make a privacy complaint on behalf of another



person if they have authorised you to do so, they are a minor/child and you are their parent or guardian, they lack capacity and you are their guardian or have other legal authority to act for them.

To make a privacy complaint about Council, you must send your complaint to Council in writing and include:

- an address for us to respond to you (e.g. an email address); and
- information about the matter or issues you are complaining about (e.g. what did the Council do or did not do with your personal information that you believe breached the QPPs and the IP Act).

Complaints should be lodged with Council within 12 months of becoming aware of the act or practice you think constitutes a breach by Council of the IP Act.

If you are lodging a privacy complaint on behalf of another individual, you must provide valid authority to act on their behalf (e.g. signed consent, power of attorney, or evidence of parental responsibility).

Submit your complaint via any of the options below;

- write to Hinchinbrook Shire Council, PO Box 366, Ingham QLD 4850; or
- email council@hinchinbrook.qld.gov.au; or
- in person at 25 Lannercost Street, Ingham QLD 4850; or
- Privacy complaint form.

Council has 45 business days to resolve the privacy complaint to the individual's satisfaction. If this does not occur, the individual can escalate the complaint in accordance with Council's Complaints Management Policy. The complaint will be managed in the same way as complaints about other areas of Council's service delivery and will be dealt with by an officer who was not involved in handling the initial complaint or the activities the subject of the initial privacy complaint. If an individual is still not satisfied with the outcome of the internal review, the complaint may be escalated to the Office of the Information Commissioner (OIC).

When assessing a privacy complaint, Council will consider all relevant information, take reasonable steps to understand the circumstances of the alleged breach, and provide the individual with a written outcome explaining Council's findings and any actions taken. Council will handle all privacy complaints confidentially and in accordance with the principles of natural justice.

5.9 Human Rights

Council is committed to respecting, protecting and promoting human rights. Council has an obligation under the *Human Rights Act 2019* to give proper consideration to human rights when making a decision, and to act and make decisions in a way that is compatible with human rights.

To the extent that an act or decision under this policy may engage human rights, Council will have regard to the *Human Rights Act 2019* in undertaking the act or making the decision.

6. Relevant Legislation

- *Information Privacy Act 2009*;
- *The Information Privacy and Other Legislation Amendment Act 2023 (IPOLA Act)*
- *Right to Information Act 2009*;
- *Human Rights Act 2019 (QLD)*
- *Public Records Act 2023*; and
- *Local Government Act 2009*.



7. Associated Documents

- Data Breach Policy;
- Records Management Framework Policy;
- Right to Information Policy and Procedure;
- Privacy and Confidential Information Management Procedure;
- Privacy Statement;
- Records Management Policy and Procedures;
- Human Rights Policy;
- Code of Conduct; and
- Councillors Code of Conduct.

DOCUMENT HISTORY AND STATUS			
Policy Number	791	Version	2
Approved By	Council Resolution # 3062026-12	Approval Date	30 June 2026
Initial Date of Adoption	29 August 2023	Next Review Date	June 2028
ECM Number	2598083	Document Contact	Business Services Coordinator