Logan City Council

Information Privacy Procedure

Logan City Council
2025

Document Control

File:	860146-1	Document ID:	13315310

Amendment History

Version Number	Description of Change	Author / Branch	Date
1.0	Creation	Corporate Governance	4 December 2019
2.0	Amendment	Corporate Governance	15 December 2025

Table of Contents

1. Procedure Objective

Logan City Council is committed to:

- Handling all personal information in compliance with the requirements of the *Information Privacy Act 2009* (Qld) (IP Act).
- Managing all access applications for information in its possession or control in accordance with the *Right to Information Act 2009* (Qld) (RTI Act).

This Procedure aims to:

- Describe how Council meets its obligations under the IP Act and RTI Act.
- Provide a guideline for Councillors and Council employees who deal with personal information in relation to the functions and activities of Council.
- Illustrate Council's commitment to respecting the privacy rights of Councillors, Council employees and members of the public.

2. How Council manages personal information

Council manages the personal information it holds in accordance with the IP Act and the Queensland Privacy Principles (QPPs) contained within.

There are 13 QPPs covering the following areas:

- Consideration of personal information privacy (QPPs 1 & 2)
- Collection of personal information (QPPs 3 – 5)
- Dealing with personal information (QPPs 6 – 9)
- Integrity of personal information (QPPs 10 & 11)
- Access to, and correction of, personal information (QPPs 12 & 13)

Reasonable steps will be taken to implement practices, procedures and systems to ensure that Council:

- Complies with the QPP's and any relevant QPP Code.
- Can respond to inquiries and complaints about privacy.

The steps Council takes will be monitored to ensure that they are effective and comply with Council's obligations under the IP Act.

To ensure that Council understands the personal information it holds and manages it in accordance with our statutory obligations, a Council wide Personal Information Holdings is maintained by the Integrity and Information Program (IIP). This register regulates the collection, use, disclosure and storage of personal information by requiring justification from the relevant business areas and overall approval by IIP. Approval by IIP must be obtained before implementing the chosen method of collection.

For more information about how Council manages personal information, visit our website www.logan.qld.gov.au/privacy

3. Situations where the IP Act may not apply

Council assesses each situation individually and maintains a on a case-by-case basis and keeps record of its evaluation and decision with regard to non-compliance.

3.1 Exemptions and permitted situations

In some circumstances, the IP Act recognises that it is appropriate to create a number of exceptions to and exemptions from the obligation to comply with the QPPs. These can be found throughout the Act, including but not limited to:

- Schedule 1 – Outlines documents that are exempt from the QPP requirements
- Schedule 3 – Exemptions are found within the QPP's themselves
- Schedule 4 – Permitted situations where the QPP's don't apply

Where the IP Act is not applicable to a document, they may have secrecy or confidentiality obligations set out in other relevant legislation.

Council will evaluate each situation on a case-by-case basis and keep record of its evaluation and decision.

3.2 Serious threat to life, health and safety

Where staff genuinely believe that there is an immediate threat to an individual's physical safety, the Queensland Police will be contacted by calling 000.

If a threat is identified, but it does not appear to be immediate, Council may still contact the relevant police service and seek advice regarding assessment and management of the threat. Usually, this will be the Queensland Police, and they will be contacted by calling Policelink on 131 444. When seeking advice on the threat, Council will not disclose personal information until we are satisfied that it is necessary as a result of the advice and in accordance with the IP Act.

Council will evaluate each situation on a case-by-case basis and keep a record of its evaluation and decision in Council's incident management system.

3.3 Law enforcement permitted non-compliance

When Council is acting as a law enforcement agency, the IP Act permits non-compliance with certain privacy principles in specific circumstances and where it is 'reasonably necessary'. There are a number of criteria set out in the IP Act which must be met before Council relies on the permitted non-compliance.

Council will evaluate each situation on a case-by-case basis and keep a record of its evaluation and decision.

3.4 Self-published personal information

Where personal information has been self-published by an individual, Council may not be required to adhere to some of the requirements of the IP Act.

4. Kinds of personal information collected and held by Council

Council conducts a diverse range of functions crucial to the provision of services to Logan City. The collection of personal information is a central part of many of these activities. The personal information Council will collect about an individual depends on the nature of the individual's dealings with Council.

Personal information held by Council includes, but is not limited to:

- Details including previous names, address history, date of birth and marital status
- License and permit information
- Financial information
- Digital photographs
- CCTV footage
- Aerial footage
- Audio and/or visual recordings
- Complaint details

4.1 Sensitive information

Council collects personal information that may be considered 'sensitive' when it is necessary to perform our functions or where required by law. Sensitive information that may be collected by Council includes, but is not limited to:

- Racial or ethnic origin
- Religious beliefs or affiliations
- Criminal records
- Health records
- Biometric information

5. Collecting personal information

5.1 How Council collects personal information

5.1.1 QPP 2 – Anonymity and Pseudonymity

Individuals will be provided the option to not identify themselves or to use a pseudonym when dealing with Council.

In each service, Council will provide an avenue for these options to be offered unless we are required by law to deal with an identified individual or where it is impractical to do so under the IP Act.

If an individual submits an anonymous customer request or a customer request using a pseudonym, and there are insufficient contact details (such as a phone

number or email address) it may not be possible for Council to complete the request. Therefore, individuals will be adequately advised of the possible consequences of using anonymity or pseudonymity, and in particular how to effectively communicate with us when using those options to ensure they still receive a high level of service.

5.1.1 QPP 3 – Solicited Personal Information

The way information is collected will always be lawful and fair. Personal information will only be collected directly from an individual unless we are exempt from doing so under the IP Act. Where required, Council will obtain consent to collect personal information.

5.1.2 Unsolicited Personal Information

If unsolicited personal information is received, an assessment will be conducted within a reasonable timeframe to determine if Council had the ability to collect it in accordance with QPP 3. Information that could not have been collected in accordance with QPP 3 will be destroyed or de-identified if it is not contained in a public record and it is lawful to do so.

Council may use or disclose personal information in order to conduct this assessment. If unsolicited information is retained, Council will ensure that QPPs 5 to 13 are complied with.

5.1.3 QPP 5 – Notice of Collection

Council will take reasonable steps when collecting information to notify or make an individual aware of:

1. Council's identity and contact details
2. If Council has collected information from someone other than the individual, Council will provide them with the circumstances of the collection.
3. If collection is required or authorised by law
4. The purposes for which Council collects the information
5. The main consequences if we do not collect the information
6. Usual disclosures made
7. Council's Information Privacy Policy provides information regarding the collection and amendment of information as well as how to submit a relevant complaint
8. Whether the information is likely to be disclosed outside of Australia and to whom

Council takes steps to ensure that the notice we provide is, with some exceptions, created using the same methodology to ensure that they are uniform and easy to understand. Council may meet some collection notice requirements through providing a link to our privacy webpage.

5.1.4 QPP 10 – Quality of personal information

When corresponding with an individual, Council will take steps to check that the information and subsequent customer record are accurate, up to date, and complete.

5.2 Purpose Council collects personal information

5.2.1 QPP 3 – Solicited Personal Information

Personal information will not be collected unless it is reasonably necessary to carry out one of Council's functions.

5.2.2 QPP 5 – Notice of Collection

Each notice of collection is specific to the method and function we are carrying out. Council will include in the notice the purpose for which the information is being collected.

5.2.3 QPP 10 – Quality of personal information

Customer information records are centralised to ensure that contact details are accurate, up to date and complete. Contact details contained in the customer information records are used by all areas of Council to conduct business and provide services.

5.3 General methods Council uses to collect personal information

Council uses a variety of different methods, software and programs to collect personal information.

5.3.1 Email

When an individual emails Council, personal information of the individual is collected and retained where necessary in accordance with relevant legislation. If an individual wishes to use a pseudonym when emailing Council, the individual must state this in the email so that Council can correspond with the individual accordingly. When using a pseudonym, an individual should ensure that the email address and information provided to Council does not contain identifying information.

5.3.2 Telephone

When an individual telephones Council, the personal information provided may be collected and retained where necessary in accordance with relevant legislation.

Council collects an individual's phone number through the customer service phone system by automatically recording the phone number of the caller against the call record. An individual may choose to block the number of the mobile phone to prevent Council's system from automatically retaining it.

If an individual calls Council to lodge a customer request, and their phone number is recorded against the call record, it may still be possible for Council to lodge the customer request without attaching the phone number or other personal information to the customer request. Council should only link the personal information obtained during the telephone call to the customer request if the customer approves the linkage or if there is a legal requirement to do so.

5.3.3 Social media

Council has official social media accounts established to reach and engage with audiences within the community. Any information provided on Council's social media sites will only be used to perform our functions or activities. The information provided to us on these platforms is collected and retained in line with

Council's record keeping obligations. Council will not send personal details to any third parties without the individual's consent, unless required or authorised to do so by law. Users of these accounts must be aware of the individual social media site's terms of use and privacy conditions prior to use.

5.3.4 Mobile apps

Mobile applications or 'apps' are software programs designed to run on a smartphone, tablet computer or other mobile device. Council currently has a range of mobile apps that are capable of capturing personal information such as location, device or contact details. Personal Information that is collected via applications are only used by Council for the purpose it was collected and managed in accordance with the IP Act. Users must be aware of the application's terms and privacy conditions prior to use.

5.3.5 Cookie data

Cookies are typically used to 'remember' the preferences of a device user and to analyse and improve our systems. Cookies are unable to access information on a device. Examples of cookies Council uses include:

- **Session Cookies** are deleted after each visit to Council's websites. Session cookies do not collect identifying information. They allow individuals to navigate and use the site's features and functionalities.
- **Preference Cookies** are used to remember an individual's preferences and various settings.
- **Security Cookies** are used for security purposes.

Council may use cookies to record anonymous, non-personal information about a person's visit to the Council website. Further information such as browsing activities may be collected including the pages visited, tools used and other such data. Council includes information about the cookies used on the respective websites. Third-party applications such as YouTube, LinkedIn or other transactional services that are embedded in Council's website may have their own cookies. Council has no direct control over the collection of information by these third-party applications.

5.3.6 CCTV

Council uses CCTV (closed-circuit television) systems in many locations throughout the city to support:

- Council functions and activities.
- Queensland Police Services (QPS) and other agencies maintain public safety.

Cameras are only installed in public spaces where public safety and/or crime is a proven concern and where infrastructure and technology permits. Council has checks in place to ensure that cameras are not deployed in spaces where a reasonable person expects to have privacy.

The Logan Safety Camera Program (LSCP) cameras are monitored 24/7 by licensed operators, specially trained staff and QPS within a central control room. The operators proactively observe images, detect incidents, and notify QPS if necessary.

Any time a CCTV captures pictures or video footage of an identifiable individual, it is potentially capturing personal information. Council's CCTV systems are operated with respect for people's privacy, and the images captured by the CCTV are maintained in the following manner:

- Access is only provided to authorised persons.
- The recording and retention of images are undertaken fairly and lawfully.
- Recorded images are only used for the purpose for which the CCTV system was installed, unless these images are required by a law enforcement agency.
- Individuals are made aware through various mechanisms that they are subject to CCTV surveillance, unless the system is being used for investigation or other law enforcement purposes.

Council makes use of the LSCP as a key component of Council's holistic approach to community safety as allowed by Council's Safety Camera Policy. These cameras are used for the dominant purpose of:

- Public safety
- Public officer disciplinary matters
- Supporting QPS in identifying and prosecuting offenders
- Effectively managing Council locations and assets

There are 2 types of Safety Cameras:

- **Overt Safety Cameras** are noticeable and located along Council owned land. The fixtures and fitting may blend in with the surroundings or environment but will remain noticeable. The locations of these cameras have been made available on Council's website.
- **Covert Safety Cameras** are relocatable cameras used by Council and other law enforcement agencies to investigate and prosecute civil and criminal offences. The location of these cameras is not available to the public due to the nature of their purpose. The cameras are not deployed in spaces where a reasonable person expects to have privacy, including public bathrooms, changeroom facilities, outdoor shower facilities, or near the windows of privately owned homes.

5.3.7 Body Worn cameras and audio recording devices

Council's compliance officers may use body worn cameras (BWCs) and/or audio recording devices when they are carrying out functions as a 'law enforcement agency' as defined by the IP Act.

Implementation of these devices for law enforcement activities have demonstrated benefits including:

- health and safety of authorised officers
- improvements in customer experience through a reduction in response time for complaint management as accessibility to image and voice data reduces the time associated with investigating complaints
- improvements in the efficiency of digital evidence management
- moderated behavior of people present at incidents
- improved officer conduct and professionalism

Council is committed to treating personal information with respect and, as such, compliance officers will only record images and sounds when exercising a legislative power. Typically, recording devices will not be left on continuously and are intended to only capture specific incidences. This approach will reduce intrusion, and the unnecessary capture of personal information of individuals who are not involved with the enforcement action.

5.3.8 Drone recording devices

Council's officers use remotely piloted drones in many locations throughout the city for law enforcement, marketing, emergency and disaster management, infrastructure assessments and environmental monitoring.

Any time a drone captures still picture or video footage of an identifiable individual, it is potentially capturing personal information. Council's compliance officers ensure that imagery is not recorded in circumstances where a reasonable person would expect to be afforded privacy. Council ensures that all drone flights are safely conducted in a manner that is consistent with the Civil Aviation Safety Authority (CASA) Rules for drone operation (Civil Aviation Safety Regulations 1998).

Council has implemented measures to ensure that the use of drones for law enforcement activities is limited to only what is necessary to carry out the law enforcement function.

Council's drones will operate in a manner that ensures:

- recording and retention of images are undertaken fairly and lawfully
- the recorded images are used only for the purpose for which the drone was operational, unless these images are required by a law enforcement agency
- individuals are made aware, where relevant, that Council operates drones
- incidental and inadvertent capture of information is limited

5.3.9 Service providers

Council uses contracted service providers to perform various functions for the community. In order for the provider to carry out these services, they may be required to collect and use personal information on Council's behalf. Council ensures that it retains control of the information by requiring providers to meet our privacy requirements. This is achieved through contractual terms which obligate service providers to adhere to certain provisions of the IP Act.

6. Holding personal information

6.1 How and why Council holds personal information

6.1.1 QPP 11 – Security of personal information

Reasonable steps will be taken to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. If the original purpose for collection is completed and the information is not required to be retained by law, Council will take steps to ensure the information is destroyed or de-identified.

6.2 General methods Council uses to hold personal information

The methods Council uses to hold personal information imposes on internal staff terms, conditions, controls, policies and frameworks to ensure that personal information is appropriately protected. Council may, from time to time, retain or require technical assistance for systems that have been developed through third parties. In this circumstance, Council ensures that appropriate controls are in place to ensure that we have ultimate control of the information is secured.

6.2.1 Hardware, assets and local servers

Council uses various corporate systems and devices that are portable or housed locally within the City of Logan. Council ensures that they are subject to the appropriate technical and physical safeguards.

6.2.2 Cloud computing

Cloud computing is a term for moving functions from a computer and agency-owned server to an online environment, usually as a solution for the storage, management, and processing of data. When using cloud-based computing systems to hold personal information, Council ensures that appropriate measures are implemented to retain control over the data.

6.2.3 Corporate systems

Council uses a variety of systems to carry out its functions. These core corporate systems include:

- **TechOne** – is a cloud based system used across Council to carry out functions for the community as well as internally for our staff.
- **Pathway** – is an onsite and cloud based business system that is primarily used to provide services to the community. The Pathway system connects to various other systems used by Council as a data source. Pathway has 3 main applications:
    - Pathway Desktop Application – which is only accessed by Council employees, for example when you lodge a customer request.
    - Epathway – is a customer self-service system located on Council's website.
    - Mobility Apps – is a mobile device tool available through the 'City of Logan' app.

- **City Maps** – is a Geographic Information System (GIS) that utilises the data in Council's Pathway system to support various functions and services.
- **eDocs (DM)** – is Council's current document management system.

7. Using and disclosing personal information

7.1 How and why Council uses and discloses personal information

7.1.1 QPP 6 – Use and disclosure of personal information

Council collects personal information for a particular purpose and in most circumstances may only use the information for that purpose. Council will take reasonable steps to advise individuals of the purpose at the time the information is collected. Information will only be used for a secondary purpose where consistent with the requirements of the IP Act.

7.1.2 QPP 10 – Quality of Personal Information

Council will only use or disclose what is relevant and necessary to fulfil the purpose we are carrying out. Before use or disclosure, Council will take reasonable steps to ensure that the information is accurate, up to date, complete and relevant.

7.2 General ways Council uses and discloses personal information

7.2.1 Use and disclosure where authorised or required by law

The information Council collects and holds will be managed in accordance with the IP Act. It is acknowledged that Council may be required to disclose information where required by statute or where it is necessary to provide a person with natural justice. If Council uses or discloses information for law enforcement purposes, a notation will be made.

7.2.2 Disclosure of personal information outside Australia

Council adheres to section 33 of the IP Act when disclosing personal information outside of Australia. For overseas based service providers, Council must be reasonably satisfied that the vendor service will manage the personal information in a matter consistent with the protections provided in the QPPs. Council ensures that appropriate privacy assessments are conducted prior to the transfer of personal information outside of Australia.

Council ensures that only the appropriate employees have the power to approve the disclosure of personal information overseas.

7.2.3 Information Sharing Agreements

Council uses personal information to deliver services and carry out functions for the community. This means that data sharing with other entities is inevitable or mandatory in some cases. Data sharing leads to better supported decisions and improved service delivery. Council utilises various Agreements and Memoranda of Understanding to facilitate this. Council takes a coordinated approach to ensure there are appropriate governance controls and oversight of all agreements to reduce the risk of duplication, inappropriate sharing of data or information being misused.

7.2.4 Artificial Intelligence

Council employs artificial intelligence (AI) technologies to enhance customers' experience, improve service delivery, secure information and for other business-related purposes. Council uses purpose-built systems that are AI integrated to collect information and prior to its use, Council ensures that the appropriate assessments and checks are undertaken.

8. Information Privacy Complaints

8.1 Making a privacy complaint

If an individual believes that Council has not dealt with their personal information in a manner that is consistent with their expectations and requirements of the IP Act, a privacy complaint can be made within 12 months of the event. Council may have the discretion to agree to an extension of this 12 month period, if it is reasonable in the circumstances.

A privacy complaint can be made in relation to a failure to comply with:

- The Queensland Privacy Principles
- Any relevant QPP code applicable to Council
- The Mandatory Data Breach Notification Scheme in Chapter 3A

There are some circumstances where a privacy complaint cannot be made. These circumstances may include personal information to the extent that it is in a document that the IP Act does not apply to, or where it is held by a bound contracted service provider. In this circumstance, Council will advise you of this and where applicable refer you to the correct entity.

8.2 How to make a privacy complaint

Privacy complaints made to Council must:

- Be in writing
- Include an address of the complainant
- Give particulars of the act or practice which is the subject of the complaint

Privacy complaints can be submitted by post, email, in person at our service centres or over the telephone. Reasonable help will be provided where required to assist individuals in putting their privacy complaint in writing.

Privacy complaints may be marked Private and Confidential and forwarded to:

Integrity & Information Program

Corporate Governance Branch

Logan City Council

PO Box 3226

LOGAN CENTRAL QLD DC 4114

Email: council@logan.qld.gov.au

Phone: 07 3412 3412

8.3 How Council deals with privacy complaints

Complaints will be acknowledged in writing within 5 business days from the date the complaint is received. Once investigated a decision will be made as to whether the complaint is substantiated within 45 business days.

If a longer period of time is required in order to finalise a complaint, the complainant will be contacted with a view to keeping the complainant informed of progress. On completion, the complainant will be advised in writing of Council's decision, including any remedies that are considered appropriate to resolve the complaint.

Where a privacy breach is identified, Council will take reasonable steps to review, implement or update practices, procedures and systems to mitigate the risk of recurrence of the breach.

9. Access to information

9.1 How Council provides access to information

9.1.1 Informal requests

QPP 12 creates a general obligation for Council to facilitate an individual accessing their personal information. Individuals can apply for access to documents containing their personal information held by Council as described through the Administrative Access to Information Policy and Procedure. Access requests through the policy are not guaranteed and may be refused if they are not suitable for informal release.

9.1.2 Formal Requests

Section 23 of the RTI Act states that a person has a right to be given access to Council documents, subject to the provisions of the Act itself.

For an access application to be valid, it must be accompanied by the application fee. There is no application fee for access applications that solely request access to the applicant's personal information.

The access application must:

- Be in writing
- Have sufficient detail to allow document identification
- State an address to which notices may be sent

Access applications for documents containing personal information of the applicant, the application must also include:

- Evidence of applicant identity
- Evidence of agent authority (if applicable)

Council will release information in accordance with the relevant legislation and may refuse access to certain types of information that Parliament has considered to be exempt or because its release would be contrary to the public interest.

10. Correction of personal information

10.1 How Council corrects personal information

10.1.1 Informal Requests

QPP 13 creates a general obligation for Council to facilitate the correction of your personal information. In most cases, an informal request will be applicable, for example, where you wish to update your contact details.

10.1.2 Formal requests

Section 78C of the RTI Act allows an individual the right to amend particular documents held by Council to the extent they contain personal information that is inaccurate, incomplete, out of date or misleading.

There is no fee associated with applications to amend an individual's personal information.

The application for amendment must:

- Be made in writing
- Have sufficient detail to allow document identification
- State an address to which notices may be sent
- Be accompanied by evidence of applicant identity
- Be accompanied by evidence of agent authority (if applicable)
- State the way in which the applicant claims the information is inaccurate, incomplete, out of date, or misleading
- If the information is claimed to be inaccurate or misleading – state the amendments the applicant claims are necessary for the information to be accurate or not misleading; and
- if the information is claimed to be incomplete or out of date – state the other information the applicant claims is necessary to complete the information or bring it up to date

Written notice of the decision regarding the application will be provided to the applicant. Amendment of a document will be made by alteration or notation on the document.

11. Information Privacy and Right to Information enquiries

All enquiries relating to Information Privacy and Right to Information are handled by Council's Integrity and Information Program and can be made in the following ways:

Post:

Integrity & Information Program
Corporate Governance Branch
Logan City Council
PO Box 3226
LOGAN CENTRAL QLD DC 4114

Email: council@logan.qld.gov.au

Phone: 07 3412 3412

If you are not comfortable using Councils general contact details, the Integrity and Information Program can be contacted directly through:

Email:

Phone:

12. Roles and Responsibilities

Role	Responsibilities
CEO	Has designated 'roles and responsibilities' for managing information privacy within Council and is the accountable officer for ensuring Council's administrative procedures and management of information practices adhere with privacy obligations.
Integrity & Information Program	The Integrity and Information Program (IIP) is responsible for managing privacy compliance, reporting, and providing advice to members of the public and employees about Council's privacy obligations. • Ensuring employees have access to adequate training materials and procedural standards in relation to privacy compliance • Delegated authority to investigate and make decisions about all privacy complaints and breaches of privacy • Providing feedback and recommendations to relevant Branch Managers when a breach of privacy has been substantiated • Leading the management of suspected and confirmed data breaches • Assisting business units in conducting privacy assessments when designing and implementing new or changed ways of handling personal information • Creation of a proactive system of privacy review

	• Reviewing and assessing Privacy Impact Assessments completed by Council staff • Maintaining a record of Council's personal information holdings • Providing advice on data sharing agreements of Council • Maintaining the Information Privacy Policy and Procedure
Executive General Managers	Executive General Managers are responsible for embedding privacy throughout their respective directorates. This includes but is not limited to: • Promoting effective privacy culture by demonstrating a best practice • Reinforcing Council's privacy expectations through awareness • Referring potential privacy issues to IIP • Raising insufficient privacy practices, procedures and systems within their directorate for review
General Managers	General Managers are responsible for privacy compliance within their respective Branch. This includes, but is not limited to: • Ensuring employees are educated about their privacy obligations • Ensuring employees follow Council's Information Privacy Policy and all associated privacy procedures and systems that are implemented by the Governance Branch in ensuring Council fulfils our legal obligations under the IP Act • Referring all privacy related matters, breaches, and complaints to IIP • Implementing practices, procedures and systems that support Council to uphold the requirements of the IP Act • Seeking advice from Corporate Governance when considering new or changed ways of handling personal information • Seeking advice from Corporate Governance on Data Sharing Agreements of Council • Facilitating regular and, where necessary, responsive privacy assessments and evaluations • Following, where relevant, obligations relating to Council's Data Breach Response • Ensuring that the appropriate checks and assessments have been completed for new and changed ways of dealing with personal information • Managing any non-conformity to Council's statutory and policy obligations by following Council's disciplinary procedures where necessary
Councillors and Council employees	Councillors and Council employees must ensure that personal information is managed in accordance with Council's privacy obligations.

	This is including, but not limited to: • Exercising due care when handling or using information acquired in their role • Reporting all suspected or actual data breaches promptly to IIP for investigation in accordance with the policy • Treating personal information with respect and exercising due care when accessing, using, handling, storing, and disposing of personal or confidential information acquired within their role • Ensuring that all personal information is properly safeguarded at all times • Avoiding the discussion of personal information with any third party • Refraining from the use of personal information to gain improper advantage for any person, entity, organisation, or themselves • Not using personal information to cause harm or detriment to Council, any person, entity, or organisation • Avoiding the access or attempt to access personal information that is not required for their role • Ensuring that they do not prevent the valid disclosure of personal to any person, entity, or organisation • Monitoring the effectiveness of privacy related controls and where necessary seeking advice • Completing Privacy Impact Assessments and implementing relevant recommendations • Conducting and seeking advice to complete the appropriate checks and assessments for new and changed ways of dealing with personal information

13. Definitions

Term	Definition
Councillor	All elected representatives of Council including the Mayor.
Personal Information	Information or an opinion about an identified individual or someone who is reasonably identifiable, whether true or not, and whether recorded in material form or not.
Identified individual	An identified individual is someone whose identity can be revealed from the information itself and includes information like a name, phone number or email.
Reasonably identifiable	An individual is ‘reasonably identifiable’ when information can be linked together to reveal their identity.

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. Routine personal work information applies to all employees not limited to those employed under the *Public Service Act 2008* (Qld). 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. The disclosure of this class of information would not give rise to a breach of the employee's privacy. 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 an author of a report • A professional opinion given wholly in a professional capacity • A position classification, for example, "planning officer" 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	Information or an opinion, that is also personal information 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 about the individual, genetic information about the individual 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.