APPLIES TO ADMINISTRATIVE POLICIES ONLY

This an official copy of the **Information Privacy Policy**, made in accordance with the provisions of *Local Government Act 2009, Local Government Regulation 2012, Information Privacy Act 2009, Right to Information Act 2009* and current Council Policies. The **Information Privacy Policy** is approved by the Chief Executive Officer of Mount Isa City Council as an **Administrative Policy** for the operations and procedures of Council.

This Policy serves as employee instruction and is not a policy adopted by Council resolution. This policy is managed by the Chief Executive Officer and distributed to employees for their instruction.

.....
Tim Rose
Chief Executive Officer

DOCUMENT VERSION CONTROL				
Governance/Policies/Administrative Doc ID# 13017			**POLICY TYPE**	Administrative
VERSION	**DATE**	**AUTHORISING OFFICER**	**DETAILS**	
V1	04.06.2013	Chief Executive Officer	**Responsible Officer –** Senior Records Officer	
V2	21.12.2023	Chief Executive Officer	**Responsible Officer –** Senior Records Officer	
V3	29.04.2025	Chief Executive Officer	**Responsible Officer –** Coordinator Governance and Disaster Management	
V4	22.08.2025	Chief Executive Officer	**Responsible Officer –** Coordinator Governance and Disaster Management	
			REVIEW DUE	08.2028

DISTRIBUTION AND DISSEMINATION			
Internal email to all employees	X	Section meetings / Toolbox talks	X
Internal email to all councillors		Included in employee inductions	
Employee noticeboards		Uploaded to Council website	X
Internal training to be provided	X	External training to be provided	
Registered in magiQ	X		

1. PURPOSE

Mount Isa City Council ("Council") collects and manages personal information in the course of performing its activities and duties. Council respects the privacy of all the personal information it holds.

The way in which Council manages the personal information it holds is governed by the *Information Privacy Act 2009 (QLD)* ("the IP Act"). This policy outlines how Council will manage personal information in accordance with the requirements of the IP Act.

2. COMMENCEMENT

This policy will commence on and from 22 August 2025. It replaces all other policies or arrangements governing information privacy (whether written or not).

3. APPLICATION

This policy applies to employees, agents and contractors (including temporary contractors) of Council, collectively referred to in this policy as "employees" in their handling of personal information.

4. DEFINITIONS

Access – means providing an individual with personal information about himself or herself that is held by the Council. This may include allowing that individual to inspect personal information or to obtain a copy of the personal information.

CCTV System – includes any system installed by the Council to electronically record and display video or audio/video of any public place or Council facility.

Collection – means gathering, acquiring or obtaining personal information from any source and by any means.

Complainant – is the individual lodging the complaint.

Consent – in relation to solicited information, means a voluntary agreement (express or implied) to some act, practice or purpose. The individual must be adequately informed before giving consent and must have the capacity to understand and communicate their consent.

Data – the representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose.

Data Breach – as defined in Schedule 5 of the *Information Privacy Act 2009*.

Disclosure – means the release of personal information to persons or organisations outside the Council (receiving entity) where the receiving entity does not know the personal information and the Council ceases to have control over the receiving entity in relation to who will know the personal information in the future. It does not include giving individuals personal information about themselves.

Eligible Data Breach – As defined in Section 47 of the *Information Privacy Act 2009*.

Frivolous – is a complaint that has no serious purpose or value. It may have little merit and be trivial in nature.

IP Act – means the *Information Privacy Act 2009 (Qld)*

Information – Data and knowledge that is generated, collected, stored or obtained which can be shared through the act of communicating, whether verbally, nonverbally, visually, electronically or in hardcopy documents.

Permitted General Situation – As defined in Schedule 4, Part 1 of the *Information Privacy Act 2009*.

Personal Information – As defined in Schedule 4, Part 1 of the *Information Privacy Act 2009.*

Public Record – As defined in Schedule 9 of the *Public Records Act 2023*.

QPPs – Queensland Privacy Principles as defined in the *Information Privacy Act 2009*.

Receiving Officer – is the Council officer who received the initial complaint.

Sensitive Information – As defined in Section 5 of the *Information Privacy Act 2009* being a category of personal information.

Vexatious – is a complaint reasonably considered to be:

- a complaint without merit and is made with the intention of causing inconvenience, annoyance or expense to Council, or
- a complaint made maliciously to damage a person's career or reputation or reputation of Council, or
- a collusion between more than once person or complainant in an attempt to discredit or take retribution against an Officer, Councillor or Council.

5. POLICY

The IP Act sets out the ways in which Council must handle personal information in accordance with the Queensland Privacy Principles (QPPs). It also gives individuals the right to request a copy of their personal information and request for documents to be amended if they are inaccurate or out of date.

5.1 What Personal and Sensitive Information is Collected and its Purpose

Council may collect, use and hold personal information when the information is essential to provide a service or perform a function of local government as broadly described below:

- To fulfil Council's responsibilities under:
  - Chapter 2 Part 1 of the Local Government Act 2009, or
  - Other [1]Local Government Acts where responsibilities have been devolved to local government, or
  - To provide services and facilities to individuals, or
- Collection is required by law, or
- Collection is necessary to prevent or lessen a serious threat to life, health, safety or welfare of an individual, or to public health, safety or welfare, or
- Collection is necessary for the establishment, exercise or defence of a legal or equitable claim, or
- Consent is provided by the individual.

Council will only collect sensitive information when it is necessary to meets its obligations under this section. Individuals will be asked to specifically consent to the collection of sensitive information and individuals may decline to provide consent. Where sensitive information is necessary to provide a service or perform a function, individuals will be informed of any impacts that not providing the information may have.

[1] Definition of ***Local Government Acts*** has the meaning assigned in Schedule 4 of the *Local Government Act 2009*

5.2 Collection Methods and Storage

Council collects personal information through a number of mediums including:

- Forms and other written correspondence (electronic and hardcopy),
- Websites and other electronic and online platforms,
- Telephone calls,
- Closed Circuit Television (CCTV) in public spaces,
- Body worn camera footage,
- Drone or other vision and audio recording devices.

Council stores personal information in both hardcopy and electronic form. Council's hardcopy information is stores on site at Council controlled facilities except where information has been transferred to Queensland State Archives for permanent retention. Electronic data is stored on cloud-based services and databases that are within the jurisdiction of Australian law.

Council secures personal and sensitive information through:

- Assigning security classifications and password protections for information held in electronic form,
- Storing hardcopy information ins secure locations that generally require security fob or key access,
- Maintaining physical and electronic security logs to monitor access, handling and distribution of information,
- Maintaining cyber security protections and controls and testing/evaluating their effectiveness regularly,
- Providing training for Council staff on privacy obligations and responsibilities.

Council has responsibility under the *Public Records Act 2003* to retain 'public records', which may include personal information, for nominated periods of time. Council endeavours where possible, at the end of the retention period, to take reasonable steps to ensure records containing personal information are securely destroyed, de-identified or the information placed beyond use.

5.3 Use and Disclosure

Where an individual provides personal information to Council, Council will inform the individual how the information will be used in a collection notice[2].

Where secondary use of the information is proposed, individuals will be asked to consent to any secondary use and will be advised of any potential impacts should consent not be provided.

There are some circumstances whee Council is required, or may use personal information collected, for purposes other than for its primary purpose, which does not require individuals to consent to its secondary use. These circumstances include:

- Where an individual would reasonably expect use/disclosure for the secondary purpose and that purpose is related to the primary purpose of collection, or in the case of sensitive information, directly related to the primary purpose,
- The secondary use of disclosure is required or authorised by, or under the laws of Australia or a court or tribunal order,

[2] As defined in the *Information Privacy Act 2009*.

- A permitted general situation exists in relation to the secondary use or disclosure,
- There is a reasonable belief that the secondary use or disclosure is necessary for one or more enforcement related activities conducted by or on behalf of, a law enforcement agency,
- The Australian Security Intelligence Organisation (ASIO) has asked the agency to disclose the personal information,
- The secondary use or disclosure is necessary for public interest research or statistical purposes.

Examples

Council meetings are legislatively required to be open to the public and therefore information on Council agendas is publicly available. The personal information of individuals will be excluded from agendas where it is not required or nor relevant for Council decision making. However, there will be circumstances where the personal information of individuals will be disclosed as part of Council meetings for example in the event of livestreaming of Council meetings.

In a disaster or emergency event, Council may pass on the personal information of individuals to other emergency service agencies for emergency response purposes.

The Planning Act 2016 requires that Council publish online, the names of development proponents and submitters at certain points of the development application process.

5.4 Access to and Correction of Personal Information

Individuals may request access to their personal information held by Council. Access will be provided subject to any restrictions that may apply under the *Information Privacy Act 2009* or *Right to Information Act 2009*.

Where an individual considers that their personal information is inaccurate, out of date, incomplete or misleading, they may lodge a request to Council for the information to be corrected, updated or additional information added.

During the course of business, where there are reasonable grounds to indicate that personal information may be incorrect, Council may take steps in consultation with the individual, to ensure that the information is corrected and/or updated.

Council does not conduct any routine monitoring of the accuracy or currency of personal information and individuals should, and in some instances are legislatively required to, contact Council when personal information changes.

Examples

Under the Animal Management (Cats and Dogs) Act 2008 the owner of a registered dog is legislatively required to advise Council of a change of address.

5.5 Transfer of Personal Information outside Australia

In complying with its obligations under s33 of the IP Act, Council will transfer an individual's personal information to someone outside Australia only if:

- the individual agrees to the transfer, or
- the transfer is authorised or required by Law, or
- Council is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health 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 a 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 transfer is necessary for the performance of Council's functions in relation to the individual
- the transfer is for the benefit of the individual and it is impracticable to seek their consent, but if it were practicable, the individual would be likely to consent
- Council has taken reasonable steps to ensure that personal information it transfers will not be held, used or disclosed by the recipient in a way that is inconsistent with the QPPs.

5.6 Contracted Service Providers

Council will take all reasonable steps to ensure that contracted service provider comply with the requirements of the IP Act (Chapter 2, Part 3) when they are provided with, or collect, personal information in order to provide services on the Council's behalf.

6. PRIVACY AND DATA BREACHES

Council will maintain a Data Breach Incident Response Plan to manage actual or suspected data breaches.

In the event that a data breach occurs, Council will apply the following strategy:

- Initial identification and evaluation of suspected breach and/or breach report
- Contain the breach or suspected breach to minimise harm
- Mitigate harm which may result from the breach including a plan to contain and mitigate any ongoing obligations which continue while the breach is being managed
- Assess and evaluate the information involved and any associated risks including assessment of whether the breach is an eligible data breach
- Notify individuals[3] of the breach or suspected breach where reasonably practicable[4], including the mandatory notifications to the Queensland Information Commissioner for eligible data breaches
- Post incident review and evaluation to inform improvements and preventative actions moving forward.

7. HOW DO I MAKE A COMPLAINT

Individuals that have concerns about personal information held by Council can lodge a complain in accordance with Council's Complaints Policy or alternatively lodge a complaint with the Queensland Information Commissioner.

7.1 VARIATIONS

Council reserves the right to vary, replace or terminate this policy from time to time.

8. ASSOCIATED LEGISLATION AND POLICIES

Local Government Act 2009

Local Government Regulation 2012

[3] Includes 'affected individuals' as defined under the *Information Privacy Act 2009*
[4] Where it is not 'reasonably practicable' a website notice will be published in accordance with the *Information Privacy Act 2009*

Information Privacy Act 2009

Information Privacy Regulation 2009

Right to Information Act 2009

Right to Information Regulation 2009

Human Rights Act 2019

Confidentiality Policy

Complaints Policy

Code of Conduct for Employees