Information Privacy Policy and Plan

Policy No:	GOV - 023
Council Resolution Ref:	120/26
Date Adopted:	21 April 2026
Review Date:	
Version No:	1
Responsible Officer:	CEO

Heads of Power

Information Privacy Act 2009 (Qld)

Privacy Act 1988 (Cth)

Information Privacy and Other Legislation Amendment Act 2023 (Qld)

Intent

This policy outlines Murweh Shire Council's (**Council**) commitment to managing personal information responsibly and in accordance with the *Information Privacy Act 2009* (Qld) (**IP Act**), as amended by the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (**IPOLA Act**). It also details procedures for handling data breaches under the Mandatory Notification of Data Breach (**MNDB**) scheme.

Scope

This policy applies to all Council employees, contractors, and agents of Council who collect, access, or manage personal information in the course of their duties.

Definitions

Data Breach: Unauthorised access to, or disclosure of, personal information, or a loss of personal information that the Council holds.
MNDB Scheme: A framework requiring agencies to notify affected individuals and the Officer of the Information Commissioner (**OIC**) about data breaches that are likely to result in serious harm.
Personal Information: Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual or an individual who is reasonably identifiable.

Policy Statement

Council is committed to protecting the privacy of individuals by ensuring that personal information is:

- Collected only when necessary for Council functions and activities.
- Stored securely to prevent unauthorised access, modification, or disclosure.
- Used and disclosed only for the purposes for which it was collected, unless otherwise authorised by law.
- Accurate, complete, and up to date.
- Accessible to individuals upon request, with provisions for correction if necessary.

Collection of Personal Information

Council will collect personal information in a lawful and fair manner, directly from individuals where possible. At the time of collection, Council will inform individuals about:

- The purpose of collection
- Any lawful authority for the collection
- Any third parties to who the information is usually disclosed.

Storage and Security

Council will take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification, or disclosure. This includes implementing physical, electronic, and managerial procedures to safeguard information.

Access and Amendment

Individuals have the right to request access to their personal information held by Council and to request corrections if the information is inaccurate, incomplete, or out-of-date. Requests will be handled in accordance with the IP Act.

Use and Disclosure

Council will only use personal information for the purpose for which it was collected, unless:

- The individual has consented to another use.
- It is required or authorised by law.
- It is necessary to prevent or lessen a serious threat to life, health, safety, or welfare.

Mandatory Notification of Data Breaches (MNDB)

In accordance with the MNDB scheme, effective from 1 July 2026, Council will:

- **Identify and Assess:** Promptly assess suspected data breaches to determine if they are likely to result in serious harm.
- **Notify:** If a data breach is likely to result in serious harm, Council will notify affected individuals and the OIC as soon as practicable.
- **Mitigate:** Take steps to contain the breach and prevent future occurrences.

Council will develop and implement a Data Breach Response Plan to ensure preparedness and a swift response to data breaches.

Responsibilities

- **Councilors and Employees:** Must adhere to this policy and related procedures.
- **Managers:** Ensure staff are aware of and comply with this policy.
- **Chief Executive Officer:** Oversee Council's compliance with privacy obligations, including the MNDB scheme.

Related Documents

- Public Interest Disclosure Policy
- Records Management Policy
- Information Security Policy
- Fraud and Corruption Prevention Policy
- Data Breach Response Plan

Document Controls

This policy will be reviewed every two years or as required by changes in law or best practice.

Policy Owner

Legal and Governance.

Approval

Chief Executive Officer			
Date:	xx/03/2023	Signature:	

INFORMATION PRIVACY PLAN

Introduction

A key aspect of democratic governance is the responsible handling of personal information and Murweh Shire Council (**Council**) is strongly committed to protecting the individual's right to privacy and protecting the personal information of individuals.

The *Information Privacy Act 2009* (Qld) (**the Act**) gives an individual the right to access and amend any of their personal information that is held by Council.

Obligations about the collection, use, storage and disclosure of personal information are provided in the Information Privacy Principles (**IPPs**) contained in the Act. The eleven IPPs appear in Appendix "A" of this Information Privacy Plan (**Plan**).

Under the Act personal information held by Council must be responsibly and transparently collected and managed (including the transfer of personal information held by Council to other agencies, other levels of Government and to the community or private sector) in accordance with the IPPs.

The Act also provides a complaint mechanism for any act or practice thought to be in breach of the IPPs.

The Plan aims to assist members of the public in understanding how their personal information is managed within Council and to assure members of the public that their personal information is being managed in accordance with the Act. The Plan will also assist persons who deal with personal information and provide a strategic overview for achieving compliance with the Act.

Application of this Plan

The Plan applies to:

- all Councillors and Council employees; and
- contractors and consultants engaged by Council.

When dealing with personal information, the Councillors and Council employees must comply with the IPPs.

Council regularly enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on behalf of Council. The Act requires personal information to be managed in accordance with the IPPs and, in regard to any outsourcing arrangements, contracts and licences entered into, Council will take all reasonable steps to ensure contractors agree to comply with the IPPs.

Where Council has partnership agreements with companies or individuals, Council must also take all reasonable steps to bind the companies or individuals to the IPPs.

Personal information

What is personal information?

Personal information is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Examples of personal information include a person's name and address, signature, email address, date of birth, driver licence number and physical characteristics such as height, birthmarks and tattoos.

Personal information also includes information about a person's political and religious beliefs, psychological profile, medical records, disabilities and sexual preferences.

Information does not need to explicitly identify a person for it to be characterised as personal information. The information needs only to provide sufficient information to lead to the identification of a person. Personal information is not limited to confidential or sensitive personal details, and it covers information held in paper or electronic records, including images and sounds.

What is not personal information?

The IPPs do not apply to information that is publicly available, for example, information in Council's land record, white pages, electoral rolls, annual reports and the Queensland Government Gazette.

Documents

The IPPs do not apply to a document to the extent it contains personal information:

Covert activity

- arising out of or in connection with a controlled operation or controlled activity within the meaning of the *Police Powers and Responsibilities Act 2000* (Qld) or the *Crime and Corruption Act 2001* (Qld) (**the CCC Act**);
- arising out of or in connection with a covert undertaking of an operation, investigation or function of a law-enforcement agency;
- obtained under a warrant issued under the *Telecommunications (Interception and Access) Act 1979* (Cth);

Witness protection

- about a witness who is included in a witness protection program under the *Witness Protection Act 2000* (Qld), or who is subject to other witness protection arrangements made under an Act;

Disciplinary actions and misconduct

- arising out of a complaint made under Part 7 of the *Police Service Administration Act 1990* (Qld);
- arising out of a complaint or an investigation of corruption under the CCC Act;

Public interest disclosures

- contained in a public interest disclosure under the *Public Interest Disclosure Act 2010* (Qld) (**the PID Act**); or
- that has been collected in an investigation arising out of a public interest disclosure under the PID Act.

Additionally, the IPPs do not apply where the:

- authority to collect, use, store and disclose personal information has an overriding statutory base;
- personal information is that of a deceased person; or
- personal information is in a generally available document.

Classes of personal information held

Council holds a range of documents that contain personal information. These documents may include:

Operational documents

- internal and external correspondence
- application forms
- telephone recordings
- complaints
- inspection record, including photographs
- receipts and invoices
- customer requests
- purchase orders
- compliance and penalty notices
- transaction histories

Personnel records

- recruitment records
- attendance and overtime records
- medical records
- tax file number declaration forms
- personal history files
- performance appraisals
- trade, skill and aptitude tests
- travel documentation
- contracts and conditions of employment
- leave applications and approvals
- payroll records
- declarations of pecuniary interests
- education records
- personal development and training records
- personal welfare records

Other records

- records of accidents and injuries, including compensation and rehabilitation case files
- records relating to disciplinary matters, including records of complaints, grievances and investigations
- recommendations for honours and awards
- CCTV footage and photographic imagery

These classes of personal information are examples only and it is not intended to represent an exhaustive list. Council may hold other classes of personal information.

Responsibilities for privacy within Council

The overall responsibility for privacy in Council rests with the Chief Executive Officer. Council employees have a responsibility to ensure they comply with the Act. All Councillors and

The day-to-day management of privacy has been delegated to the Manager Legal Services who is responsible for reporting privacy matters to the Chief Executive Officer.

Council's Legal Services Department is the first point of contact for members of the public, Councillors and Council employees, on privacy matters, including:

- breach of privacy complaints;
- requests for internal reviews of decisions relating to privacy and personal information;
- requests from individuals for the amendment of their personal information in Council's records; and
- general information on privacy in Council.

The Legal Services Department can be contacted by email at mail@murweh.qld.gov.au or by phone on (07) 4656 8355.

Public registers managed within Council

Council is required to keep certain public registers which may contain personal information. Details of the registers are available on Council's website.

Access and amendment procedures

Under the Act, a person has a right to request access to or amendment of their personal information. Applications for access to, or amendment of, personal information must be dealt with through the existing

Right to Information and Information Privacy process. Details of this process are available on Council's website at Right to Information | Shire of Murweh.

Complaint process

If a person believes that Council has not dealt with their personal information in accordance with the IPPs, they may make a complaint to Council. If Council does not respond to the complaint within 45 business days of receiving the complaint, or the complainant considers the response to be inadequate, they may make a written complaint to the Information Commissioner.

Complaints or enquiries about privacy should be directed to the below address:

Post: PO Box 63, Charleville, Qld, 4470

Email: mail@murweh.qld.gov.au

APPENDIX A

Information Privacy Principle 1 - Collection of personal information (lawful and fair)

(1)

An agency must not collect personal information for inclusion in a document or generally available publication

unless –

(a)

(b) the information is collected for a lawful purpose directly related to a function or activity of the agency; and

the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.

(2)

An agency must not collect personal information in a way that is unfair or unlawful.

Information Privacy Principle 2 - Collection of personal information (requested from individual)

(1)

This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies only if the agency asks the individual the subject of the personal information for either –

(a)

(b) the personal information; or

information of a type that would include the personal information.

(3)

The agency must take all reasonable steps to ensure that the individual is generally aware of –

(a)

(b) the purpose of the collection; and

if the collection of the personal information is authorised or required under a law –

(i)

(ii) the fact that the collection of the information is authorised or required under a law; and

the law authorising or requiring the collection; and

(c)

(d) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the first entity) -- the identity of the first entity; and

if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the second entity) – the identity of the second entity.

(4)

The agency must take the reasonable steps required under subsection (3) –

(a)

(b) if practicable – before the personal information is collected; or

otherwise – as soon as practicable after the personal information is collected.

(5)

However, the agency is not required to act under subsection (3) if –

(a) (b)

(c)

call or during the giving of treatment or assistance to a person in need of an emergency service;

the personal information is collected in the context of the delivery of an emergency service; and

the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and

the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

Example –

Personal information collected during a triple 0 emergency

Information Privacy Principle 3 - Collection of personal information (relevance etc.)

(1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies to personal information only if the agency asks for the personal information from any person.

(3) The agency must take all reasonable steps to ensure that –

(a) the personal information collected is –

(i) relevant to the purpose for which it is collected; and

(ii) complete and up to date; and

(b) the extent to which personal information is collected from the individual the subject of it and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

Information Privacy Principle 4 - Storage and security of personal information

(1) An agency having control of a document containing personal information must ensure that –

(a) the document is protected against –

(i) loss; and

(ii) unauthorised access, use, modification or disclosure; and

(iii) any other misuse; and

(b)

if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.

(2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

Information Privacy Principle 5 - Providing information about documents containing personal information

(1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out –

(a) whether the agency has control of any documents containing personal information; and
(b) the type of personal information contained in the documents; and
(c) the main purposes for which personal information included in the documents is used; and
(d) what an individual should do to obtain access to a document containing personal information about the individual.

(2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

Information Privacy Principle 6 - Access to documents containing personal information

(1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.

(2) An agency is not required to give an individual access to a document under subsection (1) if –

(a) the agency is authorised or required under an access law to refuse to give the access to the individual; or
(b) the document is expressly excluded from the operation of an access law.

Information Privacy Principle 7 - Amendment of documents containing personal information

(1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information –

(a) is accurate; and
(b) having regard to the purpose for which it was collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.

(2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.

(3) Subsection (4) applies if –

(a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and
(b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).

(4)

The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

Information Privacy Principle 8 - Checking of accuracy etc. of personal information before use by agency

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used; the information is accurate, complete and up to date.

Information Privacy Principle 9 - Use of personal information for relevant purpose

(1)

This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.

(2)

The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

Information Privacy Principle 10 - Limits on use of personal information

(1)

An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless –

(a)

the individual the subject of the personal information has expressly or impliedly agreed to the use of

(b) the information for the other purpose; or

the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to

(c) public health, safety or welfare; or

use of the information for the other purpose is authorised or required under a law; or

(d)

the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for one or more of the following by or for a law enforcement agency –

(i)

the prevention, detection, investigation, prosecution or punishment of criminal offences

(ii) or breaches of laws imposing penalties or sanctions;

(iii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iv) the protection of the public revenue;

(v) the prevention, detection, investigation or remedying of seriously improper conduct;

the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(e)

the other purpose is directly related to the purpose for which the information was obtained; or

Examples for paragraph (e) –

1. An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.

2.

An agency uses personal information, obtained for the purposes of operation core services, for the purposes of planning and delivering improvements to the core services.

(f)

all of the following apply –

(i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest; (ii) the use does not involve publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information; (iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

(2) If the agency uses the personal information under subsection (1)(d), the agency must include with the document a note of the use.

Information Privacy Principle 11 - Limits on disclosure

(1) An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the relevant entity), other than the individual the subject of the personal information, unless –

(a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is
(b) the agency's usual practice to disclose that type of personal information to the relevant entity; or
(c) the individual has expressly or impliedly agreed to the disclosure; or
the agency 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;
(d) or
(e) the disclosure is authorised or required under a law; or
the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for one or more of the following by or for a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences
(ii) or breaches of laws imposing penalties or sanctions;
(iii) the enforcement of laws relating to the confiscation of the proceeds of crime;
(iv) the protection of the public revenue;
(v) the prevention, detection, investigation or remedying of seriously improper conduct;
the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
following apply –
(f) all of the

(i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public
(ii) interest;
the disclosure does not involve the publication of all or any of the personal information in a form
(iii) that identifies the individual;
it is not practicable to obtain the express or implied agreement of the individual before
(iv) the disclosure;
the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

(2) If the agency discloses the personal information under subsection (1) (e), the agency must include with the document a note of the disclosure.

(3) If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not use or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.

(4) The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that –

(a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and
(b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and
(c) the individual has not made a request mentioned in paragraph (b); and
(d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and
(e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically.