Rural City of Wangaratta

Privacy Policy 2023

Document Type	Major Council Policy
Department	Council-wide
Date of Council Endorsement	29 September 2023
Date for Review	September 2023
Responsible Officer	Corporate Planning & Governance Specialist
Authorising Officer	Director Corporate and Leisure
Version Reference Number	2.0
SIM Reference Number	TBC

1. Statement and Purpose

1.1 The Rural City of Wangaratta (Council) is committed to ensuring that all personal and sensitive information collected by Council is handled in accordance with the requirements of the Information Privacy Principles (IPPs) as contained in the *Privacy and Data Protection Act 2014* (Vic) (the PDP Act) and is only collected, used and disclosed for its primary purpose and only for core business reasons.

1.2 This Policy relates to the collection, use and disclosure of personal and/or sensitive information by a Council representative. Third party access to personal information is captured under Council's Data Breach Policy 2021.

1.3 This Policy is administered by the Corporate Planning & Governance Specialist.

2. Scope

2.1 This policy applies to all people employed with or who undertake work on behalf of Council in any capacity, including but not limited to Council employees, Councillors, agents, contractors, members of Council Advisory Committees or Community Reference Groups and independent members of the Audit and Risk Committee.

3. Policy

3.1 In Victoria, the privacy rights of the public are protected under the PDP Act and the *Health Records Act* (Vic) ('HRA'). This policy only relates to information collected under the PDP Act; any health information captured by Council will be held in accordance with the HRA and any supporting policy.

3.2 The IPPs outline how Victorian public sector organisations must handle personal information.

3.3 Council will only disclose personal information when legally required and in accordance with all internal policies, procedures and external guidelines. As communicated in Council's Privacy Collection Statement, Council will notify all affected parties of any disclosures of their personal information.

3.4 The main purposes of the PDP Act are to:

a. provide for responsible collection and handling of personal information in the Victorian public sector;
b. provide remedies for interferences with the information privacy of an individual;
c. establish a protective data security regime for the Victorian public sector; and
d. establish a regime for monitoring and assuring public sector data security.

4. Information Privacy Principles

Principle 1 – Collection

4.1 Under IPP 1, organisations must only collect personal information necessary for a core function of that organisation.

4.2 Council will only obtain personal information for purposes relating to a specific Council purpose and will communicate the necessity of such collection to any person affected by such collection. Council will provide an opportunity for any person to remain anonymous if appropriate and practicable.

4.3 Given the breadth of Council's services, a 'specific Council purpose' will be referenced in the Privacy Collection Statement provided when Council collects that personal information.

Principle 2 – Use and Disclosure

4.4 Under IPP 2, organisations must only use and disclose personal information it has obtained for the purpose it has been collected, unless the disclosure for a secondary purpose is permitted.

4.5 **The eight secondary purposes in which Council can use or disclose the personal information include when:**

a. the individual in which the personal information relates would reasonably expect Council to release this information to a third party;
b. the individual has provided consent to release this information for a specific purpose;
c. necessary for research or the compilation of statistics;
d. necessary to lessen or prevent serious threats to health or safety;
e. investigating suspected unlawful activity;
f. required or authorised by law;
g. reasonably necessary to assist with law enforcement and/or protection of public revenue; and
h. requested to do so by a Commonwealth security agency (i.e., ASIO or ASIS).

4.6 If Council is obliged to disclose personal information to a third party under 4.4, it will provide that individual notice in writing of this disclosure, the reasons for this disclosure and any available appeal rights.

4.7 Whenever disclosing personal information under clauses 4.3 – 4.5 (excepting when required to do so by law), Council will ensure that the information requested by the third party is being requested for legitimate reasons and will be recorded by that third party securely.

Principle 3 – Data Quality

4.8 Under IPP 3, organisations must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate and complete and remains current.

4.9 Council will verify the personal information it obtains, including preferred method of contact, and ensure that any information on Council's information system is reflective of this verification.

4.10 Council will ensure that all personal information is maintained in accordance with its Information Retention and Disposal Policy and Information and Records Management Policy.

Principle 4 – Data Security

4.11 Under IPP 4, organisations must take reasonable steps to protect the personal information it possesses from misuse and loss and from any unreasonable access, modification or disclosure and to destroy or permanently de-identify personal information if it is no longer required.

4.12 Council's Information and Records Management Policy and Information Management and Retention Policy outlines Council's commitment to the integrity and security of personal information.

Principle 5 – Openness

4.13 Under IPP 5, organisations who obtain and/or use personal information must have a written policy about its management of personal information.

Principle 6 – Access and Correction

4.14 Under IPP 6, organisations who hold the personal information of individuals must make that information accessible to the person in which that information relates, unless:

a. providing access would pose a serious threat to the safety of that person or another person;
b. the disclosure would unreasonably breach the privacy of another person;

c. the request is frivolous or vexatious;
d. the information relates to legal proceedings;
e. providing access would be unlawful;
f. denying the request is authorised by a relevant law; or
g. granting access would prejudice an investigation of a possible unlawful event.

4.15 If Council cannot provide a person access to their personal information, it will identify ways, if possible, of providing sufficient information to satisfy both parties and will inform the individual in writing of why access cannot be granted in full.

4.16 All individuals maintain the ability to correct any personal information that Council has in its disposal at any time.

Principle 7 – Unique Identifiers

4.17 Under IPP 7, organisations must not apply unique identifiers to any personal information it obtains, unless that unique identification assists that organisation in achieving its core business functions.

4.18 Council will only provide a unique identifier when Council must communicate with the community on a matter and, for practical reasons and to protect the identity of a person, bulk communications are identified as the preferred method.

Principle 8 – Anonymity

4.19 Under IPP 8, organisations must allow individuals the opportunity to not identify themselves wherever lawful and practical in the circumstances.

4.20 Council recognises that individuals may wish to remain anonymous. Council will endeavour to ensure that anonymity is protected whenever necessary but there may be some occasions when anonymity cannot be ensured (for example, rates notices or when a customer requests a call back when making a complaint or request).

4.21 In the event anonymity is not a practical option, Council will ensure all personal information is de-identified.

4.22 If personal information cannot be de-identified, Council has an information management policy framework in place to ensure access is only granted to Council employees who require access and access is only provided for the reasons in which the information was obtained.

Principle 9 – Transborder Data Flows

4.23 Under IPP 9, Council must ensure that any personal information it collects remains subject to all applicable privacy provisions once that information is transferred outside of Victoria.

4.24 Council will ensure that it exercises all due diligence in any situation in which the personal information it collects is disclosed to an interstate or international entity. The due diligence includes but is not limited to requesting evidence of any privacy policy of the organisation requesting the personal information and a rationale as to why the information is being sought.

Principle 10 – Sensitive Information

4.25 Under IPP 10, Council must not collect any sensitive information, unless a customer has given express consent for the collection of this information or if the collection of this type of information is required or authorised by law.

5. Roles and Responsibilities

5.1 **Council** representatives must comply with this policy when managing the personal information of any person. Any uncertainty regarding the release of any personal information should be communicated to the Governance and Reporting Advisor for determination.

5.2 Council's **Governance and Reporting Advissor** is responsible for ensuring any breaches of this policy are reported to the relevant body as per the applicable legislative instrument.

5.3 Council's Governance and Reporting Advisor is responsible for ensuring the maintenance of this policy and for ensuring sufficient organisation-wide understanding of the Information Privacy Principles and the implication these Principles have on their work.

6. Breaches

6.1 Any breaches relating to the collection, use or disclosure of the private and/or sensitive information under this policy will be considered by the Corporate Planning & Governance Specialist.

6.2 Any breach in relation to the unauthorised access, modification or disclosure by third parties will be actioned in accordance with the Data Breach Policy 2021 and escalated to the applicable agency for determination.

6.3 Council's Data Breach Response Plan outlines the remedial actions available to Council in case of a breach of policy and internal procedures for managing breaches will be followed and communicated to all relevant parties.

6.4 Depending on the nature and scope of the breach, potential legal repercussions outside the scope of the policy may exist. For further guidance, Council's governance unit can provide further advice.

7. Human Rights

7.1 This policy has considered and complies with the Human Rights and Responsibilities contained in the Victorian Charter of Human Rights and Responsibilities Act 2006.

8. Gender Impact Assessment

This policy has considered and applied Council's Gender Impact Assessment Template and satisfies the provisions established in the *Gender Equality Act 2020* (Vic).

9. Monitoring and evaluation

9.1 This policy must be considered by Council's Audit and Risk Committee at least once in its three-year cycle to determine its effectiveness and scope.

10.Definitions

Core Business relates to a situation in which Council is required to obtain personal information from a community member to fulfil any legal obligations. For example, rates notices, for a period of community consultation that may have a direct impact on a person's property, to action a complaint (if applicable) etc.

Data Breach means any unauthorised access, modification or disclosure of the private or sensitive information of any person by a third party6.

Personal Information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

Primary purpose relates to the specific purpose of collecting that information. For example, if personal information is collected to ensure a missing waste bin is collected, Council must not use that personal information for another purpose, except in accordance with this policy or the Act.

Secondary purpose relates to a situation which does not relate to the primary purpose of collecting such information.

Sensitive Information means information or an opinion about an individual's— (a) racial or ethnic origin; or (b) political opinions; or (c) membership of a political association; or (d) religious beliefs or affiliations; or (e) philosophical beliefs; or (f) membership of a professional or trade association; or (g) membership of a trade union; or (h) sexual preferences or practices; or (i) criminal record— that is also personal information.

Unique Identifier means a number or letter sequence that marks that particular record as unique from every other record of its type.

11.References and Related Policies

Legislation

- *Aged Care Act 1997* (Cth)
- *Health Records Act*
- *Privacy and Data Protection Act 2012* (Vic)

External

- OVIC – *The Guidelines to the Information Privacy Principles* (November 2019)

12. Review

Version History		
Version Number	**Date of change**	**Reasons for change**
1.0	April 2018	Establishment of policy
2.0	April 2023	Standard review