

Privacy Policy

Date adopted: April 2023

Responsible Service Area: Governance and Performance

Purpose

Council is committed to fully understanding, complying with, and implementing its obligations under the *Privacy & Data Protection Act 2014* (the Act) and the *Health Records Act 2001*.

Council adheres to the Information Privacy Principles (IPPs) prescribed within the Act and the Health Privacy Principles (HPPs) as prescribed by the *Health Records Act 2001*.

This Policy aims to outline and provide guidance on the IPPs and HPPs and a statement that explains in simple language how Maroondah handles personal information.

Policy Position

Maroondah City Council (Council) is strongly committed to protecting individuals' private information as well as their right to privacy. The purpose of this policy is to establish the responsible handling of personal information, in accordance with legislative requirements, regulations, and good governance.

Scope

All Council employees, contractors and volunteers of Maroondah City Council must comply with the provisions of the Acts and this Policy.

While Council employees usually handle personal or health information, Council may outsource some of its functions to third parties (i.e. garbage collection or aged care services). This may require the contractor to collect, use or disclose certain personal or health information.

Council requires contractors to comply with the IPPs and/or HPPs and the provisions of the Acts in all respects.

Relationship to the Maroondah 2040 Community Vision

Community Outcome: A well governed and empowered community

Key Directions: Provide community inspired governance that is transparent, accessible, inclusive and accountable

Policy Control Schedule

Policy Title: Privacy Policy		Policy type: Statutory
Current version approved: 24 April 2023		Current version number: 6
		Policy review date: May 2025
Parent policy: N/A	Child policy/policies: N/A	Policy responsibility: Governance and Performance

Objectives

The objectives of the Acts and this Policy are:

- To establish a regime for the responsible collection, storage, handling, and disclosure of personal information
- Provide individuals with rights of access to information about themselves held by Council
- Provide individuals with the right to request Council correct and amend information about themselves, including information held by contracted service providers
- Balance the public interest in the right to information and the protection of privacy and personal information
- Provide remedies for interferences with the information privacy of an individual.

Policy Principles

The *Privacy and Data Protection Act 2014* prescribes ten IPPs which Council must comply with, as follows:

Information Privacy Principle 1	Collection
Information Privacy Principle 2	Use and Disclosure
Information Privacy Principle 3	Data Quality
Information Privacy Principle 4	Data Security
Information Privacy Principle 5	Openness
Information Privacy Principle 6	Access and Correction
Information Privacy Principle 7	Unique Identifiers
Information Privacy Principle 8	Anonymity
Information Privacy Principle 9	Transborder Data Flows
Information Privacy Principle 10	Sensitive Information

The *Health Records Act 2001* prescribes eleven HPPs which Council must comply with, as follows. The HPPs are similar to the IPPs, with some slight differences:

Health Privacy Principle 1	Collection
Health Privacy Principle 2	Use and Disclosure
Health Privacy Principle 3	Data Quality
Health Privacy Principle 4	Data Security and Data Retention
Health Privacy Principle 5	Openness
Health Privacy Principle 6	Access and Correction
Health Privacy Principle 7	Identifiers
Health Privacy Principle 8	Anonymity
Health Privacy Principle 9	Transborder Data Flows
Health Privacy Principle 10	Transfer or closure of the practice of a health service provider
Health Privacy Principle 11	Making information available to another health service provider

Policy implementation

Adherence to Information Privacy Principles (IPPs)

Principle 1 - Collection

Council will collect personal information that is necessary for its functions and activities. In some instances, Council is required by law to collect personal information. Council will only collect sensitive information where individuals have consented, or it is permitted under the law and specifically authorised under another Act or Regulation.

When it is reasonable and practical to do so, Council will collect personal information about an individual directly from that individual. When doing so, Council will inform of the purposes for which the information is collected and used in accordance with lawful and fair means. If Council collects personal information about an individual from someone other than the individual, Council will take reasonable steps to make the individual aware of these matters.

The types of information collected by Council may include:

- Full name
- Address
- Date of Birth
- Email address
- Phone Number
- Emergency Contact details
- Bank Account Details
- Tax File Number

Further information regarding the collection of personal information can be found within Council's Privacy Collection Notice.

Principle 2 - Use and Disclosure

Council must not use or disclose personal information for a purpose other than:

- The primary purpose for which it was collected
- A directly related secondary purpose the person would reasonably expect
- For those conditions specified in the Act
- Where the use or disclosure is specifically authorised under another Act or Regulation
- Where consent has been obtained from the individual; or
- Where it is considered reasonable to do so (i.e. ownership details under the Fences Act 1968)

Generally, Council would be 'using' personal information if Council possess control of how the information is handled. For example, if Council:

- search their records for your personal information
- access and read the personal information they hold about you
- make a decision based on the personal information they hold about you
- pass your personal information from one part of the organisation or agency to another.

Organisations to which Council may disclose personal information include but are not limited to, the Victorian Ombudsman, Office of Victorian Information Commissioner (OVIC), debt collection agencies, VicRoads, Insurers, legal advisors, contracted service providers, printer and mailing services, State Government Agencies, law enforcement bodies and courts.

In circumstances where the health or safety of a person is at risk, Council reserves the right to disclose personal information without consent if deemed reasonable.

Principle 3 - Data Quality

Council must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date. This is achieved by providing individuals the opportunity to update their personal information periodically upon contact being made with Council.

Principle 4 - Data Security

Council maintains a secure system for the storage of personal information. Technological and operational policies and procedures are in place to protect all personal information it holds from misuse, loss, unauthorised access, modification or disclosure.

Council takes all reasonable steps to lawfully and responsibly destroy or permanently de-identify personal information when it is no longer needed for any purpose, subject to compliance with the *Public Records Act 1973* or any other applicable Act or Regulation.

Principle 5 - Openness

Council must make publicly available its policies in relation to the management of personal information. On request, Council will inform individuals in general terms of the types of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information, subject to the provisions of the *Freedom of Information Act 1982* and/or any other applicable Act or Regulation.

Council achieves these objectives by making public this Privacy Policy, and Council's Part II Freedom of Information Statement.

Principle 6 - Access and Correction

If Council holds personal information about an individual, the individual has the right to request access to their own personal information, except in specific circumstances as outlined within the Act and the IPPs (e.g. where the information relates to legal proceedings).

If an individual believes that their personal information held by Council is incorrect then a request may be made to correct the information. Such a request will be handled in accordance with the provisions of the Act.

Principle 7 - Unique Identifiers

Council must not assign, adopt, use, disclose or require unique identifiers from individuals, unless necessary for efficient function, or if required by law. Council will only use or disclose unique identifiers assigned to individuals by other organisations, if the individual consents to the use and disclosure, or the conditions for use and disclosure set out within the Act are satisfied.

Principle 8 - Anonymity

Council must, where it is lawful and practicable, give individuals the option of not identifying themselves when supplying information or entering into transactions with Council.

Principle 9 - Transborder Data Flows

Council may transfer personal information outside of Victoria only if that data transfer conforms to the reasons and conditions outlined within the Act.

Principle 10 - Sensitive Information

Council must not collect sensitive information about an individual except for circumstances specified under the Act or in circumstances whereby such information is both directly pertinent and necessary to the specific, proper and legitimate functions of one or more of its activities. A situation where this may apply

could be where an individual, in need of urgent medical treatment, is incapacitated and unable to consent to the collection of their health information at that time.

Privacy Collection Notice

All Council forms that collect personal information are required to have a collection notice that will refer an individual to this policy for further information and where it can be located (Council's website).

The intention of the collection notice is to inform individuals of why Council is collecting the information, how Council will handle the information, possible ramifications of non-completion of the form, and access to the information provided.

A generic collection notice has been developed to assist all Council service areas in tailoring their notice to suit their service specific notices. The generic privacy collection notice is as follows:

"Maroondah City Council is committed to protecting your privacy as prescribed by the Privacy and Data Protection Act 2014 and the Health Records Act 2001. The information you provide on this form is being collected by Maroondah City Council for the strict purpose of conducting Council business. Your information will not be disclosed to any external party without your consent, unless Council is required to do so by law or it is part of the Council business that is being undertaken. Failure to provide the information requested may make you ineligible to receive the service or be part of an event/function that is the subject of this form. Any access to the information, amendments that may be required or any privacy enquiries may be directed to Council's Privacy Officer and Health Records Officer on 1300 88 22 33 or email - privacy@maroondah.vic.gov.au"

Privacy Concerns or Complaints

If an individual is concerned or aggrieved by Council's handling of their personal information, they may refer the matter to Council's Privacy Officer or Health Records Officer.

Such matters will be investigated within a reasonable time frame and a written response will be provided.

Alternatively, individuals may direct their concern to the Office of Victorian Information Commission (OVIC) or the Health Complaints Commissioner (HCC). Please note that the relevant Commissioner may recommend the initial complaint be made to Council in the first instance prior to conducting inquiries into the matter.

Office of the Victorian Information Commissioner (OVIC)
PO Box 24274
Melbourne VIC 3001
Phone: 1300 006 842
Email: enquiries@ovic.vic.gov.au
Website: www.ovic.vic.gov.au

Health Complaints Commissioner (HCC)
Level 26, 570 Bourke Street
Melbourne VIC 3000
Phone: 1300 582 113
Website: www.hcc.vic.gov.au

Policy Breaches

Employees who are in breach of this policy may be subject to disciplinary action, performance management and review. Serious breaches may result in termination of employment, in accordance with the Council's Discipline Policy (HR 06-02).

Data Breaches

All data breaches must be reported to Council's Privacy Officer as soon as practicable once a breach is detected via privacy@maroondah.vic.gov.au

When a data breach is reported to the Privacy Officer, a risk assessment of the breach will be conducted and determine probability of harm to any individuals whose private information may have been compromised. If there is a high probability of harm, the Privacy Officer shall promptly notify:

- (a) OVIC and/or the HCC of the breach and determine an appropriate course of action, and
- (b) Coordinator Corporate Planning, Risk and Information, Manager Governance and Performance, and the Manager Communications and Citizen Experience.

Council will, as soon as reasonably practicable, notify individuals who are deemed to be at a high risk of harm as a consequence of the data breach. Following the harm minimisation and containment phase, assessment and review will occur to investigate the circumstances and cause, with a view to prevent similar incidents in future.

The Council's Privacy Officer shall maintain a data breach register which will be used to record all known breaches.

Roles and Responsibilities

All Council employees are responsible for familiarising themselves with the Privacy Policy to ensure they comply with the IPPs and the HPPs.

The Privacy Officer is responsible for privacy matters within Council. The Privacy Officer will review the Privacy Policy every two (2) years, liaise with senior management to ensure compliance with the Act, and provide guidance and support for all Council employees. All general enquiries concerning privacy matters should be directed to the Privacy Officer at privacy@maroondah.vic.gov.au

The nominated Council role to undertake functions of the 'Privacy Officer' and 'Health Records Officer' is listed under the *Register of Delegations: S7 Instrument of Sub-Delegation by the CEO - Risk and Integrity*.

Related legislation

If a provision made by or under the *Privacy and Data Protection Act 2014* relating to an IPP or applicable code of practice is inconsistent with a provision made by or under any other Act, the other provision prevails and the provision made by or under the *Privacy and Data Protection Act 2014* is (to the extent of the inconsistency) of no force or effect.

Below is a non-exhaustive list of legislation that Council operates under:

- Aboriginal Heritage Act 2006
- Building Act 1993
- Building Regulations 2018
- Child Wellbeing and Safety Act 2005
- Children, Youth and Families Act 2005
- Children's Services Act 1996
- Disability Act 2006
- Domestic Animals Act 1994
- Emergency Management Act 1986
- Environmental Protection Act 1970
- Fences Act 1968
- Fire Services Property Levy Act 2012
- Food Act 1984
- Freedom of Information Act 1982
- Health Records Act 2001
- Independent Broad-based Anti-Corruption Commission Act 2011
- Infringements Act 2006
- Land Act 1958
- Local Government Act 1989 and the Regulations under the Act
- Local Government Act 2020 and the Regulations under the Act
- Planning and Environment Act 1987
- Public Interest Disclosures Act 2012
- Public Records Act 1973
- Road Management Act 2004
- Road Safety Act 1986
- Sport and Recreation Act 1972
- Subdivision Act 1988
- Valuation of Land Act 1960
- Victorian Civil and Administrative Tribunal Act 1998
- Victorian Inspectorate Act 2011
- Victorian Local Government Grants Commission Act 1976
- Victoria State Emergency Service Act 2005

Related policies

- Complaints Policy
- Employee Code of Conduct (HR06-06)
- Freedom of Information Part II Statement
- Information Management Policy
- Maroondah CCTV Policy
- Public Transparency Policy
- Public Interest Disclosures Act Policy
- Risk Management Policy
- Use of Body Worn Cameras by Authorised Officers Policy

Definitions

Data Breach - Information that is held by Council and is subject to misuse, loss, unauthorised access, modification or disclosure without the knowledge or authorisation of the system owner or in this case, Council.

Health Information - Under the *Health Records Act 2001*, Health Information is defined as: Information or an opinion, whether true or not, about the physical, mental, or psychological health (at any time) of an individual; the disability of an individual; an individuals expressed wishes about the future provision of health services for themselves; or information about a health service provided or to be provided to an individual. This includes other personal information collected to provide, or in providing, a health service, or in connection with the donation or intended donation by an individual of their body parts, organs or body substances. Health information can also be genetic information about an individual, that is or could be predictive of the health (at any time) of that individual or of any of their descendants.

Health Service - Under the *Health Records Act 2001*, Health Service is defined as: an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it, to assess, maintain or improve the individuals health; or to diagnose the individuals illness, injury or disability; or to treat the individuals illness, injury or disability or suspected illness, injury or disability; or a disability service, palliative care service or aged care service; or the dispensing on prescription of a drug or medicinal preparation by a pharmacist registered under the Health Practitioner Regulation National Law; or the sale or supply of a voluntary assisted dying substance within the meaning of the *Voluntary Assisted Dying Act 2017* in accordance with that Act by a pharmacist registered under the Health Practitioner Regulation National Law to practice in the pharmacy profession (other than as a student); or the supply or administration of a voluntary assisted dying substance within the meaning of the *Voluntary Assisted Dying Act 2017* in accordance with that Act by a registered medical practitioner; or a service, or a class of service, provided in conjunction with an activity or service referred to above that is prescribed as a health service- but does not include a health service, or a class of health service, that is prescribed as an exempt health service for the purpose of this Act generally or for the purposes of specified provisions of this Act or to the extent that it is prescribed as an exempt health service.

HPPs - Health Privacy Principles listed under the *Health Records Act 2001* that regulate the handling of health information.

IPPs - Information Privacy Principles listed under the *Privacy and Data Protection Act 2014* that regulate the handling of personal information.

Personal Information - Under the *Privacy and Data Protection Act 2014*, personal information is defined as 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.

Privacy Officer / Health Records Officer - The nominated Council role to undertake functions of the 'Privacy Officer' and 'Health Records Officer' is listed under the *Register of Delegations: S7 Instrument of Sub-Delegation by the CEO - Risk and Integrity*.

Public Registers - Documents that are held by Council that are open to inspection by members of the public and may also contain personal information - as is prescribed by legislation.

Sensitive Information - Council may also hold what is considered sensitive information. Sensitive information includes information or an opinion about an individual such as:

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Trade union membership
- Membership of a professional or trade association
- Religious beliefs or affiliations
- Philosophical beliefs
- Sexual preference or practices
- Criminal record