



## Privacy and Data Protection Policy

Department/Unit	Governance & Risk	First Implemented	November 2002	Review Date	May 2029
Origin	Coordinator Communications, Governance & Risk	Reviewed	March 2025	Version	7
Authorising Officer	Endorsement by Council	Effective From	21 May 2025	TRIM Reference	E513

### Purpose/Objective

Mansfield Shire Council (Council) views the protection of an individual's privacy as an integral part of its commitment to accountability and integrity in all its activities and programs.

This policy outlines Council's commitment to protecting an individual's right to privacy and the management of personal information as required by the *Privacy and Data Protection Act 2014* (PDP Act) and the *Health Records Act 2001* (HR Act).

This policy aims to:

- ▶ establish a system for the responsible collection, storage, handling and disclosure of personal information;
- ▶ provide individuals with access to information about themselves held by Council; and
- ▶ allow individuals to request correction or amendment of their personal information held by Council, including information held by contracted service providers.

### Scope

This Policy applies to both personal information and health information collected and/or held by Council. This includes personal information collected on forms, in person, in correspondence, over the telephone, from third parties, through any of Council's public access interfaces or via Council's website.

This policy applies to all Mansfield Shire Council employees, Councillors, contracted employees, volunteers and members of Committees.

## Policy Statement

Council is committed to adhering to the Information Privacy Principles (IPP), the Health Privacy Principles (HPP) and the *Privacy and Data Protection Act 2014* when undertaking statutory functions, programs and activities to protect individual privacy.

Councillors, Council officers, volunteers, contracted employees and members of Committees will observe the ten (10) IPPs and eleven (11) HPPs as required by legislation.

Information Privacy Principles	Health Privacy Principles
1. Collection	1. Collection
2. Use and Disclosure	2. Use and Disclosure
3. Data Quality	3. Data Quality
4. Data Security	4. Data Security and Retention
5. Openness	5. Openness
6. Access and Correction	6. Access and Correction
7. Unique Identifiers	7. Identifiers
8. Anonymity	8. Anonymity
9. Trans-Border Data Flows	9. Trans-Border Data Flows
10. Sensitive Information	10. Transfer/closure of the Practice of a Health Service Provider
	11. Making Information available to another Health Service Provider

### Collection (IPP 1 / HPP 1)

Council will collect personal information lawfully, fairly and only as necessary for its functions and activities. Information will be collected:

- ▶ Directly from the individual via an application form or correspondence or in response to a request from Council.
- ▶ From third parties, such as contracted service providers, health service providers or the individuals authorised representatives or legal advisers.
- ▶ From publicly available sources.
- ▶ As required by law.

Council will advise individuals, where possible, of the purposes for which their personal information is being collected and of those third parties to whom the information may be disclosed.

## Mansfield Shire Council | Privacy and Data Protection Policy

Where it is reasonable and practicable to do so, Council will collect personal and health information directly from the individual. If Council collects personal information about an individual from someone else, it will take reasonable steps to ensure that the individual is made aware of it.

Council will not collect sensitive or health related information unless:

- ▶ The individual has provided consent.
- ▶ It is required by law.
- ▶ It is required for legal claims, research or the analysis of statistics relevant to government funded community programs.
- ▶ It is necessary to prevent a serious and imminent threat to the life, health or safety.

Examples of sensitive information include:

- ▶ individuals receiving Council services related to maternal and child health, youth services, supported playgroups and integrated family services.
- ▶ personal information of employees, volunteers and contract service providers, relevant to their employment or contract with the Council.
- ▶ information pertaining to criminal record.
- ▶ Council will take reasonable steps to retain confidentiality of any personal information given in confidence about an individual, by another person or a health service provider, in relation to the provision of care or health services to the individual.

For individuals under 18 Council will obtain parental or guardian consent unless the young person is living independently or parental involvement may hinder service delivery.

### Use and Disclosure (IPP 2 / HPP 2)

Council will take all necessary measures to prevent unauthorised access to, or disclosure of personal information.

Council will only use personal information for the primary purpose for which it was collected (e.g. levying rates, billing, planning and building approvals, maternal and child health and family support services) and any related purpose the individual would reasonably expect Council to use or disclose the information to, or where the individual has consented to the use or disclosure.

The information may be disclosed:

- ▶ to Council's contracted service providers who manage the services provided by Council. Council will require these service providers to maintain the confidentiality of the information and comply with the privacy principles in all respects.
- ▶ to statutory bodies for targeted consultation (e.g. VicRoads, Goulburn Murray Water).
- ▶ to organisations and services prescribed by the Child Wellbeing and Safety (Information Sharing) Regulations as information sharing entities who are permitted to share information under the Child Information Sharing Scheme.
- ▶ to individuals for the purpose of serving a notice to fence as required by the *Fences Act 1968*.
- ▶ to the Victorian or Australian Electoral Commission for the compilation of voters rolls.

- ▶ to statutory bodies (e.g. Centrelink, Child Support) for purposes required by relevant legislation.
- ▶ where appropriate under another Act, including *Freedom of Information Act 1982*.
- ▶ to emergency agencies (eg, Victoria Police, Australian Federal Police, fire department(s) or State Emergency Service) for emergency or law enforcement purposes.
- ▶ in public registers that need to be maintained in accordance with other Acts, as a release of information relevant for the purpose for which the registers exist.
- ▶ to an individual's authorised representatives, health service providers or legal advisers.
- ▶ to Council's professional advisers, including accountants, auditors and lawyers.
- ▶ to organisations assisting Council to perform statistical analysis for improving the services being delivered to the community. However, where practicable and reasonable, steps will be taken to de-identify the information.
- ▶ to an immediate family member of the individual for emergency reasons or if it is necessary to provide the appropriate care or health service to the individual.
- ▶ to a recipient outside Victoria only if they are governed by substantially similar privacy principles or the individual has consented to the transfer or would be likely to give it, if it was practicable to obtain that consent.
- ▶ when legally compelled to do so (e.g. Under direction of a court order).

### Data Quality (IPP 3 / HPP 3)

Council will take reasonable steps to ensure that all personal information collected, used or disclosed is accurate, complete and up to date

### Data Security and Retention (IPP 4 / HPP 4)

Council will take all necessary measures to maintain a secure system for storing personal information and will utilise appropriate technologies, security methods, operational policies and procedures to protect the information from unauthorised access, improper use, alteration, unlawful or accidental destruction and accidental loss.

Council will dispose of personal information, where it is no longer necessary to fulfil the purposes for which the information was collected or as required by law, in accordance with the *Health Records Act 2001* and the *Public Records Act 1973*.

### Openness (IPP5 / HPP 5)

This policy details Council's management of personal, sensitive and health information and is publicly available for viewing on Council's website.

On request, Council will take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

A collection notice will be provided to clients by Council services and programs, where appropriate, to inform them of how the service handles personal and health information and Applicable legislation includes the Privacy and Data Protection Act 2014 (Vic), the Health Records Act 2001 (Vic), the Children, Youth and Families Act 2005 (Vic), the Family Violence Protection Act 2008 (Vic) and the Child Wellbeing and Safety Act 2005 (Vic).

### Access and Correction (IPP 6 / HPP 6)

Individuals may request access to or correction of their personal information on written request to the most relevant Council department or to Council's Privacy Officer (Coordinator Customer Service & Information Management), except in specific circumstances as outlined within the *Privacy and Data Protection Act 2014* and the *Freedom of Information Act 1982*.

Council will take reasonable steps to correct personal information that is inaccurate, incomplete or out-of-date.

If access or correction of personal information needs to be denied Council will give the individual the reasons for that decision as soon as practicable. Reasons to deny access or correction may include:

- ▶ required by law or relates to legal proceedings.
- ▶ release would pose a serious threat to the life or health of any person.
- ▶ is classified as confidential information.

Council officers from time to time may contact individuals to confirm that the information held is correct via telephone, mail or email to ensure Council is meeting its obligations under IPP 3 - Data Quality.

### Request for Information by Third Parties

All requests for personal contact details from a third party must be considered by Council's Privacy Officer.

Under the IPPs Council may disclose personal information for such a purpose as it is related to the facilitation of a statutory process and also that a resident and ratepayer might reasonably expect disclosure to be made in this instance.

With respect to IPP 4 (data security), Council is required to take reasonable steps to protect such personal information from misuse. In this context such requests must confirm the name and contact details of the organisation making the request.

A written assurance by the requesting body is required confirming that contact details will be used solely for the purpose of printing and mailing resident and ratepayer letters and notifications as part of the reason for request and that it will not be retained, copied or disseminated for unrelated purposes – see Appendix 1.

The written assurance must also confirm that Council has informed the requestor about the relevant IPPs – see Appendix 2.

## Unique Identifiers (IPP 7 / HPP 7)

Unique identifiers, such as numbers or codes, can assist with matching data. Use of unique identifiers by organisations is only allowed under certain conditions.

Council will not adopt, use, or disclose a unique identifier assigned by another government agency unless:

- ▶ the individual has provided their consent, or
- ▶ it is required or authorised by law.

## Anonymity (IPP 8 / HPP 8)

Where lawful and practicable, individuals have the right to remain anonymous when providing information or engaging in transactions with Council.

However, as anonymity may limit Council's ability to process a complaint or other matter, Council reserves the right to take no action on any matter if an individual chooses not to supply relevant personal information necessary for Council to perform its functions.

## Trans-border Data Flows (IPP 9 / HPP 9)

Council will only transfer personal or health information outside of Victoria in accordance with the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*.

## Sensitive Information (IPP 10)

Subject to exclusions contained within the Act. Council will not collect sensitive information about an individual unless:

- ▶ the individual has consented; or
- ▶ the collection is required under law; or
- ▶ the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
  - a) is physically or legally incapable of giving consent to the collection; or
  - b) physically cannot communicate consent to the collection; or
- ▶ the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

## Transfer or Closure of Health Service Provider's Practice (HPP 10)

Health information relating to a discontinued health service provided by Council will be managed in accordance with the *Health Records Act 2001*.

## Making Information Available to Another Health Service Provider (HPP 11)

If an individual:

- ▶ requests Council to make health information relating to the individual available to another health service provider; or

- ▶ authorises another health care service provider to request Council to make health information relating to the individual available to the requesting health service provider,

Council will provide a copy or written summary of that health information as soon as practicable following payment of a fee not exceeding the prescribed maximum fee and subject to the regulations.

## Privacy Statement

At times it may be relevant to include a privacy statement on a Council form or document as follows:

### **Privacy Statement**

*Mansfield Shire Council considers that the responsible handling of personal information is a key aspect of democratic governance and is strongly committed to protecting an individual's rights to privacy. Council will comply with the Information Privacy Principles and Health Privacy Principles as set out in the Privacy and Data Protection Act 2014 and Health Records Act 2001. The information received will be used for the primary purpose it was collected or any related purpose for which the individual would reasonably expect Council to use or disclose the information. The information will not be disclosed to any other party unless Council is required to do so by law.*

## External Contractors

Council may outsource some of its functions to third parties which may require the contractor to collect, use or disclose certain personal information (eg, waste collection).

Council requires all external contractors to comply with this policy and applicable legislation all respects.

## Breaches of this Policy

Unauthorised disclosure of personal data is considered a breach of this Policy and will be dealt with on a case-by-case basis.

If a breach occurs, the following four key steps will be undertaken:

1. Contain the breach and conduct a preliminary assessment
2. Evaluate the risks associated with the breach
3. Remediate and notify (and other steps to mitigate harm)
4. Review the cause of the breach and Council's response and take steps to improve practices and lessen the likelihood of future breaches.

Regardless of the cause of a suspected privacy breach OVIC encourages councils to report a breach to their office so that OVIC staff can provide guidance on containing and managing the breach. It may also be appropriate to notify the individuals whose personal information was involved in the breach, so that they can take any necessary remedial action.

Council can notify OVIC of a breach by email to [privacy@ovic.vic.gov.au](mailto:privacy@ovic.vic.gov.au) or by using the Data Breach Reporting Form on OVIC website.

## Notifiable Data Breaches Scheme

Under the Notifiable Data Breach Scheme, contained in Part IIIC of the *Commonwealth Privacy Act 1988*, Council is required to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals if there has been an 'eligible data breach' of tax file number (TFN) information.

An eligible data breach occurs when there is loss of unauthorised access to, or unauthorised disclosure of, Personal, Sensitive or Health information which is likely to result in serious harm and remedial action has not been taken to prevent such risk of harm.

Council is not otherwise directly subject to the *Commonwealth Privacy Act 1988*. However, Council may at times agree to be bound by this Act (for example, where it receives funding under a Commonwealth program).

Community service organisations funded through Department of Health (DH) and Department of Families, Fairness and Housing (DFFH) are encouraged to report early, contain and respond proportionally and identify risks and harm. DH notify the DH privacy Team at [privacy@health.vic.gov.au](mailto:privacy@health.vic.gov.au).

DFFH funded organisations, the report should be submitted through the [Feedback Management System](#). The report will be received by the privacy officer and directed to the funded organisation's contract manager within the department (i.e. the Area advisor), who will work with the funded organisation to manage the incident as required. Read more about the [Feedback Management System and Reporting incidents](#) on the Providers website.

## Privacy Complaints

Complaints, in the first instance, may be directed to Council's Privacy Officer. These complaints will be acknowledged within five business days (inline with Council's Customer Service Charter) and resolved as soon as practicable inline with Council's Complaints Handling Policy.

The complaint must be received within six months from the time the complainant first became aware of the misconduct and details of the complaint will be kept confidential at all times.

Alternatively, individuals may lodge a complaint with the Office of the Victorian Information Commissioner with respect to personal information, or the Health Services Commissioner for health information, about a Council act or practice that may be an Interference with their privacy.

### **The Office of the Victorian Information Commissioner about personal information:**

Online: [ovic.vic.gov.au](http://ovic.vic.gov.au)  
Email: [enquiries@ovic.vic.gov.au](mailto:enquiries@ovic.vic.gov.au)  
Telephone: 1300 006 842

### **The Health Complaints Commissioner about health information:**

Online: [hcc.vic.gov.au](http://hcc.vic.gov.au)  
Email: [hcc@hcc.vic.gov.au](mailto:hcc@hcc.vic.gov.au)  
Telephone: 1300 582 113

## Definitions

Term	Definition
Council	Mansfield Shire Council
Health information	Information or opinion about the physical, mental, psychological health of an individual, disability of an individual or a health service provided or to be provided to an individual, but does not include information about an individual who has been deceased for more than 30 years.
HPPs	Health Privacy Principles as set out in the <i>Health Records Act 2001</i> .
IPPs	Information Privacy Principles as set out in the <i>Privacy and Data Protection Act 2014</i> .
OVIC	Office of the Victorian Information Commissioner
PDP Act	<i>Privacy and Data Protection Act 2014</i>
Personal information	Information or opinion, whether true or not and whether recorded in material form or not, about a living individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.
Sensitive Information	Information or opinion about an individual's ethnic origins, religious beliefs, political opinions or association, philosophical beliefs, membership of professional association or trade union, sexual preferences or practices and criminal record.

## Responsibilities

Managers are responsible for ensuring their staff comply with the principles, practices and any associated procedures of this policy. Adherence to the Privacy and Data Protection Policy will be overseen by the Chief Executive Officer, with any associated procedures implemented by Council's Privacy Officer.

Council's Privacy Officer, Coordinator Customer Service & Information Management, is the owner of this Policy. Any review of this Policy must be made in consultation with the Coordinator Customer Service & Information Management.

## References / Related Policies

- ▶ *Child Wellbeing and Safety Act 2005*
- ▶ *Children, Youth and Families Act 2005*

Mansfield Shire Council | **Privacy and Data Protection Policy**

- ▶ *Criminal Act 1958*
- ▶ *Family Violence Protection Act 2008*
- ▶ *Fences Act 1968*
- ▶ *Freedom of Information Act 1982*
- ▶ *Health Records Act 2001*
- ▶ *Privacy Act 1998*
- ▶ *Privacy and Data Protection Act 2014*
- ▶ *Public Records Act 1973*
- ▶ *Workplace Injury Rehabilitation and Compensation Act 2013*
- ▶ OVIC Privacy Considerations for Local Government
- ▶ Victorian Protective Data Security Standards V2.0 (OVIC)
- ▶ Mansfield Shire Council Employee Code of Conduct
- ▶ Mansfield Shire Council Records and Information Management Policy
- ▶ Mansfield Shire Council Information Security Policy
- ▶ Model Councillor Code of Conduct

## Gender Impact Assessment

The Privacy and Data Protection Policy has considered the Gender Equality Act 2020 in its preparation but is not relevant to its content. The Policy has been assessed as not requiring a Gender Impact Assessment (GIA) as it is purely administrative in its nature and does not have the potential to influence broader social norms and gender roles..

## Implementation

This Policy is effective from 21 May 2025.

## Review Date

This Policy is to be reviewed by May 2029 unless legislative changes determine otherwise.

## Authorisation to Implement Policy

Signed:   
 \_\_\_\_\_  
 Councillor

Witnessed:   
 \_\_\_\_\_  
 Chief Executive Officer

Approval dated: 21 May 2025

**Mansfield Shire Council reserves the right to review, vary or revoke this Policy at any time.**

## APPENDIX 1: Written Assurance Form

**(THIS FORM IS TO BE PLACED ON REQUESTING COMPANY'S LETTERHEAD)**

I, \_\_\_\_\_ of \_\_\_\_\_

have read and understood the Mansfield Shire Council's Privacy and Data Protection Policy relating to the disclosure of personal contact details with respect to resident and ratepayer information.

I confirm that the disclosed information has been requested for the purposes of:

*(Please record purpose of request)*

Once signed, this document forms the written assurance required that the contact details will be used solely for the purpose outlined above and will not be retained, copied or disseminated for unrelated purposes and that Council has informed *[insert Company name]* about the relevant Information Privacy Principles.

**Signed:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Company:** \_\_\_\_\_

this \_\_\_\_\_ day of \_\_\_\_\_ 20 \_\_\_\_\_

**IN THE PRESENCE OF:**

**Witness Name:** \_\_\_\_\_

**Signed:** \_\_\_\_\_

## APPENDIX 2: Third Party Information Requested

Enquiries: [Officer Name]  
 Telephone: 03 5775 85XX  
 Our Ref: [Records Number]

[Date]

To be sent on Mansfield  
 Shire Council letterhead

Name  
 Address Line 1  
 SUBURB/TOWN/STATE/POSTCODE (ALL CAPS, NO PUNCTUATION)

Dear [Name]

### Information Privacy Principles for Ratepayer Database

The *Victorian Privacy and Data Protection Act 2014* allows for the application of Information Privacy Principles (IPPs) to guide Council in considering disclosure of personal contact details with respect to resident and ratepayer information.

It is understood that the contact information has been requested for the purposes of [*insert reason for request*].

Under the IPPs, Council may disclose personal information for such a purpose as it is related to the facilitation of a statutory process and also that a resident or ratepayer might reasonably expect disclosure to be made in this instance.

With respect to IPP 4 (data security), Council is required to take reasonable steps to protect such personal information from misuse. In this context, such requests must confirm the name and contact details of the organisation making the request. It is acknowledged that [*name of person or company*] has already provided adequate information in this respect as part of the request.

A written assurance is required that the contact details will be used solely for the purpose of printing and mailing resident and ratepayer letters and notifications as part of the [*reason for request*] and will not be retained, copied or disseminated for unrelated purposes. The written assurance also confirms that Council has informed [*name of company/person making request*] about the relevant IPPs.

I would be grateful if you could sign the attached assurance, on company name letterhead, and return it to Council at your earliest convenience. A copy of the ratepayer information will then be forwarded to you for the purposes you have stated.

Yours sincerely

**Name (bold)**  
 Privacy Officer