

Privacy and Data Protection Policy

<p>Department/Unit: Governance & Risk</p>	<p>First Implemented: 26 November 2002 Reviews: 6 March 2013 2 October 2014 30 September 2015 17 October 2017 Effective From: Immediate Review Date: February 2025 Version: 6 Trim Reference: E513</p>	<p>Origin: Coordinator Governance & Risk Endorsed by Council: 20 April 2021</p>
--	--	--

1. PURPOSE

Mansfield Shire Council views the protection of an individual's privacy as an integral part of its commitment towards 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* (PDPA) and the *Health Records Act 2001* (HRA).

This policy has been developed in order to:

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

2. SCOPE

This Policy applies to both personal information and health information collected and/or held by Mansfield Shire 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 our website.

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



3. DEFINITIONS

The 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.
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.
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.
Council	means Mansfield Shire Council
HPPs	Health Privacy Principles
IPPs	Information Privacy Principles

4. POLICY STATEMENT

The aim of this policy is to ensure that everyone handling personal data is aware of the requirements and acts in accordance with this policy.

The Council will adhere to the Information Privacy Principles, the Health Privacy Principles and the *Privacy and Data Protection Act 2014* at all times when undertaking our statutory functions and activities, so that the privacy of individuals can be protected.

This policy outlines ten (10) IPPs and eleven (11) HPPs for Councillors, Council officers, contractors, volunteers and members of Council committees to note and observe as required by legislation.

The ten Information Privacy Principles are:	The eleven Health Privacy Principles are:
<ol style="list-style-type: none"> 1. Collection 2. Use and Disclosure 3. Data Quality 4. Data Security 5. Openness 6. Access and Correction 7. Unique Identifiers 8. Anonymity 9. Trans-Border Data Flows 10. Sensitive Information 	<ol style="list-style-type: none"> 1. Collection 2. Use and Disclosure 3. Data Quality 4. Data Security and Retention 5. Openness 6. Access and Correction 7. Identifiers 8. Anonymity 9. Trans-Border Data Flows 10. Transfer/closure of the Practice of a Health Service Provider 11. Making Information available to another Health Service Provider



4.1 Collection

Council will collect personal information lawfully and fairly and only collect personal information that is necessary for its functions and activities, including:

- 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 of information
- when legally required to do so.
- as far as it is practicable to do so, Council will collect personal information about an individual directly from that individual. It will also inform the individual of the purposes for which the information is collected, whom it will be disclosed to and how he/she is able to gain access to the information.

Council will not collect sensitive or health related information unless:

- the individual has consented.
- it is required by law.
- it is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of an individual or the public.
- it is necessary for the establishment, exercise or defense of a legal claim.
- it is necessary for research, compilation and analysis of statistics relevant to government funded community programs.

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.

Upon collection Council will inform the individual:

- why the information is being collected,
- to whom the information will may be disclosed and why,
- any law that requires Council to collect the information,
- the consequences for the individual if all or part of the information is not collected, and
- the fact that he/she is able to gain access to the information.

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 collect personal information about a child under the age of 18, only with the consent of the child's parent or guardian. However, in certain circumstances Council may exercise discretion in obtaining parental/ guardian consent for the collection of young person's information where parental/guardian involvement may hinder the delivery of services to a young person. If a young person under the age of 18 years is living independently of their parents/guardian, permission to collect personal information may be provided.



4.2 Use and Disclosure

Council will only use personal information for the primary purpose for which it was collected (for example, levying rates, billing, collection of debts, property valuation, town planning and building approvals, provision of family and counselling services, community services and waste management services, enforcement activities and asset management) and any related purpose the individual would reasonably expect the 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, including, waste collection, meals preparation for aged and disability services, environmental health inspections and infrastructure maintenance. Council will also require these service providers to maintain the confidentiality of the information and comply with the privacy principles in all respects.
- to statutory bodies (eg, VicRoads, Goulburn- MurrayWater) for the purposes of targeted consultation processes on major projects that could affect residents.
- to individuals for the purpose of serving a notice to fence as required by the *Fences Act 1968*.
- to the Victorian Electoral Commission or Australian Electoral Commission for the compilation of voters rolls.
- to statutory bodies (eg, Centrelink, Child Support) for purposes required by relevant legislation.
- to Victoria Police, Australian Federal Police, fire department(s) or State Emergency Service or other appropriate agencies for emergency or law enforcement purposes only.
- where appropriate under another Act, including *Freedom of Information Act 1982*.
- 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 the 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 any 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 (eg under direction of a court order).



4.3 Quality, Security and Retention

Council will endeavour 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. Retention of information will be considered in accordance with the *Health Records Act 2001* and the *Public Records Act 1973*.

4.4 Access and Correction

Council will provide individuals with access to their personal information on written request to the most relevant Council department directly or to the Privacy Officer (Coordinator Governance & Risk), except in specific circumstances as outlined within the *Privacy and Data Protection Act 2014* and the *Freedom of Information Act 1982*.

If an individual is able to establish that the personal information is inaccurate, incomplete or out-of-date, then Council will take reasonable steps to correct the information.

If access or correction of the personal information needs to be denied, as required by law or relates to legal proceedings, or the release would pose a serious threat to the life or health of any person, or is classified as confidential information, the Council will give the individual the reasons for that decision as soon as practicable.

In the event that Council and an individual disagree about the veracity of the personal information held by Council, reasonable steps will be taken to record a statement relating to the disputed information, if requested by the individual.

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

4.5 Unique Identifiers and Anonymity

Unique identifiers, usually a number, can facilitate data matching. Use of unique identifiers by organisations is only allowed under certain conditions. Council will not adopt as its own identifier, an identifier that has been assigned by another government agency and will not use or disclose the identifier assigned to an individual by another government agency, unless the consent of the individual has been obtained or it is required by law to do so.

Where lawful and practicable, individuals may exercise the option of not identifying themselves when supplying information or entering into transactions with Mansfield Shire Council.

4.6 Trans-border Data Flows

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*.



4.7 Sensitive Information

Mansfield Shire Council will only collect sensitive information where you have consented or is it required under legislation, or sensitive information that is necessary for its functions.

For example:

- individuals receiving Council services related to maternal and child health, youth and aged and disability services, and counselling programs.
- personal information of employees, volunteers and contract service providers, relevant to their employment or contract with the Council.
- information pertaining to criminal record.

4.7 Request for Information by Third Parties

All requests for personal contact details 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 company/person making the request about the relevant IPPs – see Appendix 2.

4.8 External Contractors

While personal information is usually handled by Council staff, Council may outsource some of its functions to third parties. This may require the contractor to collect, use or disclose certain personal information (eg, waste collection). Council requires all contractors to comply with the Act in all respects.



4.9 Breaches of this Policy

Unauthorised disclosure of personal data to a third party is considered a breach of this Policy. Such breaches 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 your organisation'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 local 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 or by using the Data Breach Reporting Form on OVIC website.

4.9.1 Notifiable Data Breaches Scheme

Council holds tax file number (TFN) information about its employees. 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 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).

4.10 Privacy Complaints

Complaints, in the first instance, may be directed to the Coordinator Governance & Risk (Council's Privacy Officer). These complaints will be acknowledged within two business days and will be resolved as soon as practicable.

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.



Or you can make a complaint to:

The Office of Victorian Information Commissioner about personal information:

Online: ovic.vic.gov.au
 Email: enquiries@ovic.vic.gov.au
 Telephone: 1300 006 842

The Health Complaints Commissioner about health information:

Online: hcc.vic.gov.au
 Email: hcc@hcc.vic.gov.au
 Telephone: 1300 582 113

4.11 Further Information

Copies of this policy are readily available from Council's website, www.mansfield.vic.gov.au and from the Mansfield Municipal Office. Further information with respect to the Council's Privacy and Data Protection Policy and its handling of personal information can be obtained from Council's Privacy Officer.

5. RESPONSIBILITIES

All Mansfield Shire Council employees, Councillors, contractors, volunteers and members of Council committees are responsible for adhering to and implementing this policy.

Adherence to the Privacy and Data Protection Policy will be overseen by the Chief Executive Officer, with any associated procedures implemented by the Coordinator Governance and Risk.

Council's Privacy Officer is the Coordinator Governance and Risk, and is the owner of this Policy. Any reviews of this Policy must be made in consultation with the Coordinator Governance and Risk and Chief Executive Officer.

6. REFERENCES/ RELATED POLICIES

- *Children, Youth and Families Act 2005*
- *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*
- Victorian Protective Data Security Standards (Office of the Victorian Information Commissioner Privacy and Data Protection)
- Staff Code of Conduct
- Councillor Code of Conduct
- Records and Information Management Policy
- Information Security Policy



7. IMPLEMENTATION

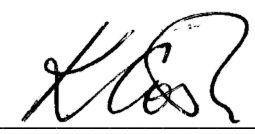
This policy is effective from 20 April 2021.

8. REVIEW DATE

This Policy is to be reviewed by April 2025 unless legislative changes determine otherwise.

9. AUTHORISATION TO IMPLEMENT POLICY

Signed: 
Councillor

Witnessed: 
Chief Executive Officer

Approval dated: 20 April 2021

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



APPENDIX 1
(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 **(please insert Company name)** about the relevant Information Privacy Principles.

Signed: _____
Name: _____
Title: _____
Company: _____

this _____ day _____ 20 _____
of _____

IN THE PRESENCE OF:

Witness Name: _____
Signed: _____



APPENDIX 2

Enquiries: **Officer Name**
Telephone: (03) 5775 8XXX

Our Ref: E

Date

Address

To be sent on
 Mansfield Shire
 Council letterhead.

Dear

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

Michelle Kain
Privacy Officer