



WARRNAMBOOL
CITY COUNCIL

PRIVACY POLICY 2025

APPROVAL DATE: NOVEMBER 2025
REVIEW DATE: NOVEMBER 2028

PRIVACY POLICY

DOCUMENT CONTROL

| | |
|-----------------------------|---------------------------|
| Document Title: | <i>POLICY</i> |
| Policy Type: | <i>COUNCIL</i> |
| Responsible Branch: | <i>EXECUTIVE SERVICES</i> |
| Responsible Officer: | <i>MANAGER GOVERNANCE</i> |
| Document Status: | <i>ADOPTED</i> |
| Approved By: | <i>COUNCIL</i> |
| Adopted Date: | <i>November 2025</i> |
| Review Date: | <i>November 2028</i> |

PRIVACY POLICY

1. INTRODUCTION

Council understands how important it is to our community's confidence in Council services to ensure that private information we hold about an individual will be treated in a way which ensures their privacy is respected and protected. Accordingly, Council is committed to full compliance with its obligations under the *Privacy and Data Protection Act 2014 (Vic.)* and the *Health Records Act 2001 (Vic.) (HR Act)*

1.1 Purpose

The purpose of Warrnambool City Council's Privacy Policy (the Policy) is to:

- Convey the principles of responsible management of personal and health information collected by Council
- Promote the protection of the privacy of individuals in all transactions with Council while ensuring a balance with the interests of Council carrying out its functions and/or activities.
- Promote responsible and transparent handling of personal information while ensuring the privacy of individuals is acknowledged and respected.
- Provide a means for individuals to make formal complaints about any alleged interference with their privacy.

1.2 Scope

This Policy applies to all Warrnambool City Council Councillors, staff, volunteers, contractors and agents and to all personal information and health information collected, used, disclosed and stored about any individual including residents, users of Council services, individuals or groups registering for any Council provided services, or those seeking employment with Council.

1.3 Definitions

| Word/Term | Definition |
|---------------------------|---|
| Agent | means an individual, member of a Council committee or an organisation employed by Council to perform a service that involves handling personal information. An agency relationship will mean that Council will usually be held responsible for how their agents (like their employees) handle personal information. |
| Council | means Warrnambool City Council |
| HRA | means the <i>Health Records Act 2001</i> |
| Health information | Includes personal information or opinion about: <ul style="list-style-type: none"> • an individual's physical, mental or psychological health (at any time) • an individual's disability (at any time) • an individual's expressed wishes about the future provision of health services to them; • health services provided or to be provided to an individual • an individual, information collected to provide a health service to them (e.g. disability and age care service, maternal and child health service, immunisation service). |

PRIVACY POLICY

| Word/Term | Definition |
|--|---|
| Health Privacy Principles (HPPs) | <p>The Health Privacy Principles (HPPs) are a set of eleven principles that regulate how health information is handled. These principles underpin the Health Act</p> <ul style="list-style-type: none"> • HPP 1 – Collection • HPP 2 – Use and Disclosure • HPP 3 – Data Quality • HPP 4 – Data Security • HPP 5 – Openness • HPP 6 – Access and Correction • HPP 7 – Identifiers • HPP 8 – Anonymity • HPP 9 – Trans-border Data flows • HPP 10 – Transfer/closure of the Practice of a Health Service Provider • HPP 11 – Making information available to another Health Service Provider |
| Information Privacy Principles (IPPs) | <p>The Information Privacy Principles (IPPs) are a set of ten principles that regulate how personal information is handled. These principles underpin the PDPA</p> <ul style="list-style-type: none"> • IPP 1 – Collection • IPP 2 – Use and Disclosure • IPP 3 – Data Quality • IPP 4 – Data Security • IPP 5 – Openness • IPP 6 – Access and Correction • IPP 7 – Unique Identifiers • IPP 8 - Anonymity • IPP 9 – Trans-border Data Flows • IPP 10 – Sensitive Information |
| Personal | means information or opinion (including information or an opinion |
| Information | <p>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 be reasonably ascertained, from that information or opinion (excluding health information)</p> <p>For example, “personal information” about an individual includes (but is not limited to):</p> <ul style="list-style-type: none"> • name; • date of birth and age • home/postal/email address and telephone number • marital status and religion • income, financial transactions, purchases and spending habits • race and ethnic origin • education • photograph and or video footage • signature |
| PDPA | means the <i>Privacy and Data Protection Act 2014 (Vic.)</i> |
| Primary Purpose | means the main reasons why the personal information was shared with or collected by Council. |
| Public Register | means documents that are open to inspection by members of the public and contain information required or permitted by legislation. |

PRIVACY POLICY

| Word/Term | Definition |
|------------------------------|--|
| Secondary Purpose | means a use or disclosure of personal information that a reasonable person would understand could occur or may occur. For example, sharing an updated mailing address on a form with all Council departments instead of remaining just with the department the form was sent to. |
| Sensitive Information | A subset of personal information. It is defined in the PDPA as information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record. |
| Delegated Committee | means a Delegated Committee of Council established under section 63 or 64 of the <i>Local Government Act 2020</i> . |

2. POLICY

This Policy has been informed by the 10 Information Privacy Principles (IPPs) contained in the *Privacy and Data Protection Act 2014*, and the 11 Health Privacy Principles (HPPs) contained in the *Health Records Act 2001*. This policy encompasses both sets of principles.

2.1 Collection

Types of Information collected by Council

Council will only collect personal and health information that is necessary for carrying out its functions and activities, and where reasonable and practicable, such information will be collected from the individual directly. However, Council reserves the right to collect personal and health information from third parties where the law or circumstances warrant it.

The collection of this information could be in various ways, including, but not limited to, the following:

- During conversations between individuals and Council representatives.
- Accessing and interacting with Council's websites or social networking sites.
- When making an enquiry, providing feedback or completing an application form (online or in hard copy).
- Through the use of Council-owned CCTV systems installed in public places for the purpose of surveillance, including cameras in or on Council property and other mobile surveillance equipment.
- The information provided may be used for purposes including (but not limited to) the following:
- To make contact where it is necessary in order to provide Council services requested by an individual.
- To make contact where it is necessary to resolve issues relating to Council services or functions.
- As part of Council's commitment to customer service, Council may periodically invite individuals to provide feedback about their experience via a voluntary survey.
- To facilitate the collection of Council fees and charges.
- To enable payment for Council provided goods and services.
- To enable Council to undertake its law enforcement functions.
- To aid community safety

PRIVACY POLICY

Collecting Photographs/Videos

Council takes photographs/videos both on Council premises and also in public places. These photographs/videos may be used for publicity or enforcement purposes.

Before taking photographs/videos to be used for publicity purposes, Council will seek consent (if practicable) from individuals to take and use the photograph(s). Where feasible, this consent will be obtained in writing.

If however, photographs are to be taken in a public place (such as at a community event) it may not be practicable to obtain individuals consent. In these instances and where practicable to do so, Council will use other methods to inform the public that photographs/videos i.e. signs and or public announcements to advise the public that photographs are being taken.

Collecting Unsolicited information

Sometimes people send personal information to Council without Council requesting it or when Council asks for some information and individuals or third parties provide more information than requested. In these circumstances where unsolicited personal information is not necessary for Council's functions, it may not be 'reasonable' to notify the individual concerned of the collection. In which case the information will simply be stored in Council's systems and disposed of in accordance with the *Public Records Act 1973*.

Collecting through Council's websites, social networking sites or SMS/MMS

If you access and interact with a Council website, social networking site or send SMS/MMS to Council we recommend you read Council's News & Social Media Policy.

Council uses social networking services, in addition to traditional methods, to connect with our community.

Council uses public social networking sites to identify social trends and issues related to Council's services and events. We use various tools to view public social media and website commentary and may engage directly with individuals who post on these sites to provide service information.

Any personal information collected by Council through these sites will be handled in line with this Privacy Policy and our News & Social Media Policy.

Collecting through Website surveys

Council uses various applications (such as SurveyMonkey®) to conduct online surveys. This means the data collected online may be stored on servers located in another country (such as the USA). To ensure that you are fully informed on how any personal information you provide in the survey will be stored, please read the privacy policy which is contained on the online survey page, prior to participating. If you do not wish to complete a Council survey online, you can request a hard copy by contacting Council's City Assist department Tel: 03 5559 4800

Collecting Online payments

You are able to make the following payments online, using Council's eService's, which in turn uses the SecurePay payment gateway to collect the credit card details and accept payment for: rates infringements/fines invoices or accounts planning, building, local laws and Infrastructure application payments animal registration renewal fees.

PRIVACY POLICY

Council does not collect or hold credit card information for these payments.

SecurePay is fully compliant with the Payment Card Industry Data Security Standard and they have direct bank links to transact. The SecurePay data is held in Australia. If you do not wish to provide this information online you should arrange to make payment by post to PO BOX 198, Warrnambool Victoria 3280, through Australia Post or in person at the Civic Centre, 25 Liebig Street, Warrnambool.

Privacy (Collection) Statement

Whenever Council collects personal information, you should be given notice of how we intend to use, share and disclose that personal information. This notice could be provided in a form similar to below:

“The personal information requested on this form is being collected by Warrnambool City Council for the purpose of [insert purpose] or any other directly related purpose. The personal information will also be disclosed to [insert names of any other entities Council will be disclosing the personal information to] for the purpose of [insert how those entities will be using the personal information]. It will not be disclosed to any other external party without your consent, unless required or authorised by law. If the personal information is not collected, [insert details of what will happen – can they still participate in the process, can they be anonymous etc.]. If you wish to alter any of the personal information you have supplied to Warrnambool City Council, please contact Council via telephone [insert number for your work area] or email [insert email address for your work area].”

2.2 Use and Disclosure

Council will only use and disclose information about an individual for:

- the primary purpose for which it was collected,
- for a secondary purpose that would be reasonably expected, or
- in other limited circumstances such as when required to do so by law.

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

Where necessary, Council may disclose your personal information to other work areas within Council to assist in actioning an enquiry.

Council also discloses personal information to external organisations such as Council's contracted service providers who perform various services for, and on behalf of, the Council. Council will ensure that these contractors agree to be bound by the provisions of the *PDPA*.

Information provided to these contractors is limited to the information required by them to provide services on behalf of Council.

Council also discloses personal information to other agencies in the course of an investigation and defense of legal claims against Council. This includes Council's professional advisors, solicitors, insurers and investigators.

Council may also use personal information contained in complaints which you make to Council as part of any prosecution undertaken as part its law enforcement functions.

PRIVACY POLICY

Where authorised, Council may also disclose personal information to:

- Debt collection agencies.
- Government agencies including the Department of Human Services, the Victorian Workcover Authority and Road Traffic Authority.
- To Police, Fire and State Emergency departments for emergency or law enforcement purposes.
- Department of Families, Fairness and Housing if required under our legislative obligations.
- Government agencies to enable them to advise you of works which may impact upon individuals or properties.
- To individuals for the purpose of serving a notice to fence as required by the Fences Act.
- Where appropriate as prescribed under another Act (e.g. the *Freedom of Information Act*) or Council is required to do so by law (e.g. to the Courts to respond to a subpoena or provide information to assist with an investigation).
- To family members, or other individuals or organisations only if Council believes that the disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare, or a serious threat to public health, safety or welfare.
- Where an individual's consent has been given.

Personal information in applications for employment with Council will be supplied to agencies such as the Victoria Police as part of a background check, or with Services Victoria as part of a Working with Children Check. The results from such checks will not be disclosed to any third party unless authorised by law or with the applicants' written authorisation.

Personal information provided as part of a public submission to a Council or Delegated Committee meeting may be included with the published agenda papers and minutes of the meeting. The published agenda papers and minutes are made available online and in hardcopy format.

Personal information may also be contained in Council's Public Registers.

In the case of health information, Council may disclose health information about someone:

- If Council is providing a health service to them and it is necessary to be able to provide that service.
- Where the person is incapable of providing consent and it is not reasonably practicable to obtain the consent of an authorised representative or the person does not have an authorised person.

Additionally there are some specific uses of personal information that may be required through Council's business areas.

Maternal and Child Health

Council provides MCH Services that are available for families with children aged 0 - 6 years. The service supports parents and offers information and advice regarding parenting, child health and development, child behaviour, maternal health and well-being, child safety, immunisation, breastfeeding, nutrition and family planning. Physical and developmental assessments of children are carried out at key developmental stages.

A variety of health and non-health information will be collected in association with MCH services including children's names, date of birth, health history, whether the child or parent is of Aboriginal or Torres Strait Islander descent, Medicare numbers, parent's health history and employment status.

PRIVACY POLICY

Health information associated with MCH will be collected for the following reasons:

- Co-ordination and provision of MCH services,
- Co-ordination of first-time parent groups, or
- To provide MCH statistics to the DHHS and other Council departments (e.g., Council's Human Services/Planning unit).

Health information associated with MCH will not be used or disclosed for a secondary purpose (i.e., other than the primary purpose) of collection unless:

- The child's authorised representative (e.g., parent or guardian) has consented to the use or disclosure of the information, or
- The secondary purpose is directly related to the primary purpose and the child's authorised representative (e.g., parent or guardian) would reasonably expect the organisation to use or disclose the information for the secondary purpose, or
- The use or disclosure is required, authorised or permitted whether expressly or impliedly by or under law (e.g., Mandatory Reporting to Child Protection Services), or
- The disclosure is reasonably necessary for a law enforcement function, or Council has reason to suspect that an unlawful activity has been or is being or may be committed and that the disclosure is necessary for an investigation or the reporting of the activity to relevant person or authorities, or
- The purpose is one of the other permitted secondary purposes listed in HPP 2.

Council may receive requests from a medical practitioner or hospital or ambulance service to obtain MCH information held by Council for a child and/or the parents/guardians. This may be in order to provide appropriate treatment for the child and/or the parents/guardians.

While this is not the primary purpose for Council's collection of the information, such a purpose may be regarded as an authorised secondary purpose under HPP 2 of the HRA.

The information can be disclosed if:

- If consent has been obtained from the child's parent or guardian, or
- If Council reasonably believes that disclosing the information to the medical practitioner/hospital/ambulance service is necessary to lessen or prevent a serious threat to the child's and/or parent's/guardian's life, health, safety or welfare.

Home and Community Care

Council provides Home and Community Care programs as part of joint Commonwealth and State Government programs that provides home support services to support elderly people, younger people with disabilities and carers.

Information associated with Home and Community Care will be collected for the following reasons:

- Assistance with everyday household and personal tasks,
- Home maintenance to client's homes by Council staff, contractors or volunteers,
- Personal and nursing care,
- Delivery of meals by volunteers,
- Allied health or paramedical services such as dietetics, occupational therapy, physiotherapy, podiatry and speech pathology,
- Group activities such as gentle exercise, gardening, craft, games and outings,
- Social support such as Telelink, regular home visits, telephone monitoring and bus transport to social activities, or
- In-home or centre-based care to provide a break for the older person or child being cared for, as well as the carer.

PRIVACY POLICY

Health information associated with HACC will not be used or disclosed for a secondary purpose (i.e., other than the primary purpose) of collection unless:

- The HACC Client or their authorised representative has consented to the use or disclosure of the information, or
- The secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or
- The use or disclosure is required, authorised or permitted whether expressly or impliedly by or under law, or
- The disclosure is reasonably necessary for a law enforcement function, or
- Council has reason to suspect that an unlawful activity has been or is being or may be committed and that the disclosure is necessary for an investigation or the reporting of the activity to relevant person or authorities, or
- The purpose is one of the other permitted secondary purposes listed in HPP 2.

Child Care Services

Child Care provide full-time and part-time care for children aged 0 - 6 years at its Child Care Centers. Information associated with Preschools and Child Care includes names and other personal information of children and their parents, as well children's health history and immunisation and medical records.

Personal and health information associated with Child Care will be collected for the following reasons:

- Administration and provision of Preschool and Child Care services,
- To provide Preschool and Child Care statistics to the DHHS and other Council departments (e.g., Council's Human Services/Planning unit),
- To meet statutory requirements (e.g., Children's Services Act 1996), and
- Administration of the Child Care Subsidy with Centrelink.

Personal and health information associated with Preschools and Child Care will not be used or disclosed for a secondary purpose (i.e., other than the primary purpose of collection) unless:

- The child's authorised representative (e.g., parent or guardian) has consented to the use or disclosure of the information, or
- The secondary purpose is directly related to the primary purpose and the child's authorised representative (e.g., parent or guardian) would reasonably expect the organisation to use or disclose the information for the secondary purpose, or
- The use or disclosure is required, authorised or permitted whether expressly or impliedly by or under law (e.g., Mandatory Reporting to CPS), or
- The disclosure is reasonably necessary for a law enforcement function, or
- Council has reason to suspect that an unlawful activity has been or is being or may be committed and that the disclosure is necessary for an investigation or the reporting of
- the activity to relevant persons or authorities, or
- The purpose is one of the other permitted secondary purposes listed in IPP 2 and HPP 2.

The *Children's Services Regulations 2020* require that Council must make available on request of a parent prescribed records relating to a child who is enrolled at the service (Part 7, Regulation 120(3)(a)). If the parent's access to information is limited by an order of a court or tribunal that is kept on the child's enrolment record, Council must refer to that order before releasing information concerning the child to that parent (Part 7, Regulation 120(3)(b).) Guardianship of the child may have been removed resulting in the non-custodial parent not having the right to seek access to the child's information, for example.

PRIVACY POLICY

In the absence of court or tribunal limitations kept on the child's enrolment record, whether Council discloses information to a non-custodial parent will be dependent on the information and circumstances of the disclosure.

Environmental Health

Council provides an Environmental Health function that seeks to prevent diseases, prolong life and promote public health through organised programs including the prevention and control of environmental health dangers, diseases, or health problems of particularly vulnerable population groups.

Some the kinds of information which may be collected includes food illness victim details, business proprietors name and addresses, records of findings against business proprietors, source of illness for food illness victims, and clinical comments made in respect to a food illness victim.

Personal and health information associated with Environmental Health will be collected for the following processes:

- Processing of food complaints,
- Notification of infectious diseases,
- Registration of premises for business,
- Register of Registration Certificates,
- Inspections/Audits of Registered Premises,
- Food sample collection and analysis, or
- Providing information associated with Registered Food Businesses to the DHHS.

Personal and health information associated with Environmental Health must not be used or disclosed for a secondary purpose (i.e., other than the primary purpose) of collection unless:

- The secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or
- The individual has consented to the use or disclosure of the information, or
- The use or disclosure is required, authorised or permitted whether expressly or impliedly by or under law, or
- The disclosure is reasonably necessary for a law enforcement function, or
- The use or disclosure is necessary to prevent or lessen a serious threat to an individual's life, health, safety or welfare or a serious threat to public health, public safety, or public welfare, or
- Council has reason to suspect that an unlawful activity has been or is being or may be committed and that the disclosure is necessary for an investigation or the reporting of the activity to relevant persons or authorities, or
- The purpose is one of the other permitted secondary purposes listed in HPP 2 or IPP 2.

2.3 Data Quality

Council will endeavour to make sure that the personal and health information it holds is accurate, complete and up-to-date. A person may request that Council amend any personal information they have provided.

2.4 Data Security

Council will take all reasonable steps to ensure personal and health information is stored safely and securely and is protected from misuse, loss, unauthorised access, modification or disclosure.

PRIVACY POLICY

Council will take all reasonable steps to destroy or permanently de-identify personal information which is no longer needed for Council purposes, subject to compliance with the *Public Records Act 1973* and the *Health Records Act 2001*.

2.5 Data Security Incident Process

In the event of data security incident the following steps will be taken:

Step 1 — Identify & Report (Immediate)

- Report suspected breaches promptly to the Manager Governance.
- Preserve evidence; avoid altering affected systems beyond agreed containment.

Step 2 — Contain (Immediate to 4 hours)

- Take reasonable steps to stop further unauthorised access, modification or disclosure (e.g., access revocation, isolation, halt outbound transmissions).
- For mis-sends/unintended disclosures, seek secure deletion/return.

Step 3 — Assess IPP/Privacy impacts (within 24 hours)

- Identify the categories of personal and sensitive information involved.
- Determine which IPPs may be engaged (security, use/disclosure, access/correction, etc.) and whether the incident likely constitutes an “interference with privacy” under the PDP Act.
- Assess whether affected data is held, processed or accessible outside Victoria.
- Check whether any information is (or could be) held or accessible outside Victoria.

Step 4 — Notification Decision & External Reporting

- Determine whether the incident meets OVIC’s threshold for notification under the Information Security Incident Notification Scheme (i.e. business impact level (BIL) 2 or higher, or adverse impact on confidentiality, integrity, availability)
- If the threshold is met, notify OVIC “as soon as practicable and no later than 30 days” of detection, using the prescribed form, updated as more information becomes available
- If the incident involves Commonwealth-governed personal information (e.g. TFNs) and triggers the Notifiable Data Breaches (NDB) scheme, assess whether mandatory reporting to OAIC is required
- Keep written record of the decision (notify / not notify) and rationale (including factors weighed)

Step 5 — Communication to Affected Individual

- Decide whether to notify affected individuals, balancing risk of harm, practicability, and community expectations.
- If notifying, prepare a clear and timely notification letter or email including:
 - What happened
 - What personal information was involved
 - What the organisation is doing to address the breach
 - Advice on steps individuals can take to mitigate risk
 - Contact details for further inquiries
- If declining to notify individuals, document reasons (e.g. low risk of harm, inability to identify recipients).
- In consultation with legal/advice, consider offering assistance (e.g. credit monitoring, identity protection services) where risk is substantial.

PRIVACY POLICY

Step 6 — Remediation, Recovery & Mitigation

- Implement remedial actions to mitigate ongoing risk (e.g. patch vulnerabilities, change passwords, upgrade encryption, improve controls, staff training).
- Recover or restore systems and data (including backups), ensuring integrity and minimal disruption.
- Validate that affected systems are secure before returning to full operation

2.6 Openness

This policy serves as Council's public commitment to openness in the management of personal information.

This policy is available in both electronic (on Council's website www.warrnambool.vic.gov.au) and hardcopy format.

Council will, on request, take reasonable steps to provide individuals with general information on the types of personal and health information it holds and for what purposes and how it collects, holds, uses and discloses that information.

2.7 Access and Correction

Should an individual wish to access their personal information, the individual can contact the most relevant Council department directly or Council's FOI/Privacy Officer (PO Box 198, 25 Liebig Street, Warrnambool. Vic., 3280 | Email: contact@warrnambool.vic.gov.au | Tel: 1300 003 280 or (03) 5559 4800.

Access will be provided except in the circumstances outlined in the Act, for example, where the information relates to legal proceedings or where the Freedom of Information Act 1982 applies. If an individual believes that their personal information is inaccurate, incomplete or out of date, the individual may request Council to correct the information. The request will be dealt with in accordance with the Act.

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/HPP 3 - Data Quality.

2.8 Unique Identifiers

A unique identifier is a number or code that is assigned to someone's record to assist with identification e.g. a drivers licence number. Unique identifiers may be assigned where necessary to enable Council to carry out any of its functions efficiently. An example is the unique identifier assigned to customers who access Council's libraries or aquatics service.

2.9 Anonymity

Where lawful and practicable, Council will give individuals the option of not identifying themselves when entering into transactions with Council. However anonymity limits Council ability to process a complaint or other matter. Therefore, if a person chooses not to supply personal information that is necessary for Council to perform its functions, then Council reserves the right to take no further action on the matter.

PRIVACY POLICY

2.10 Trans-Border Data Flows

IPP9 of the PDPA does not prohibit the transfer of personal information outside of Victoria but it does place restrictions on when it can occur. This is because the PDPA is a Victorian law and therefore the IPP's will not apply to organisations in a different state, territory or country. Council will only transfer personal or health information outside of Victoria in accordance with the provisions outlined in the PDPA and HRA.

While Council uses cloud computing services based outside Victoria, it has taken all reasonable steps to ensure that the information which it transfers will not be held, used or disclosed by the host of the information inconsistently with the Victorian IPPs. It also ensures the hosts/recipients are subject to laws and/or binding contractual arrangements that provide similar protections to that afforded under the PDPA and HRA.

2.11 Sensitive Information

Unless prior consent has been obtained from individuals in writing, or Council is required to do so by law/and or to prevent harm, Council will not collect sensitive information as defined by this Policy.

2.12 Transfer or closure of health service

Health information relating to a discontinued Council health service will be managed in accordance with the HRA.

2.13 Making information available to another health service provider

Council will provide a copy, or written summary, of health information in its possession where it is requested in writing by the individual, or by a health service provider authorised by the individual.

3. PRIVACY COMPLAINTS

If an individual is dissatisfied with Council's handling of their personal or health information, they may make a complaint to:

Manager Governance
Warrnambool City Council
PO Box 198, 25 Liebig Street, Warrnambool. Vic., 3280
Phone: 1300 003 280 or (03) 5900 4800

A complaint will be investigated in a timely, fair and reasoned way and a written response will be provided. All complaint details will be handled with discretion and confidentiality.

Alternatively, people can complain to:

The Office of Victorian Information Commissioner (OVIC), regarding personal information online or via email: www.ovic.vic.gov.au or privacy@cpdp.vic.gov.au or telephone 1300 006 842 or the Health Complaints Commissioner regarding health information, telephone 1300 582 113 or via www.hcc.vic.gov.au.

PRIVACY POLICY

OVIC provides independent oversight of the Victorian public sector's collection, use and disclosure of public sector information. OVIC's functions under the PDP Act include:

- promoting awareness and understanding of the Information Privacy Principles (IPPs);
- receiving complaints about possible breaches of the IPPs by the Victorian public sector;
- conducting audits to assess compliance with the IPPs;
- undertaking research, issuing reports, guidelines and other materials with regard to information privacy;
- developing the Victorian Protective Data Security Framework;
- issuing protective data security standards and promoting their uptake by the Victorian public sector;
- conducting monitoring and assurance activities to assess compliance with those standards; and
- undertaking research, issuing reports, guidelines and other materials with regard to information security.

3.1 Policy Owner & Review

The owner of this policy is the Chief Executive Officer. All enquiries regarding this policy should be initially directed to the Governance Manager.

This Policy will be reviewed in 2026, or as legislation requires, or Council determines a need has arisen.

3.2 Policy Compliance Responsibilities

- 3.2.1 The Chief Executive has the ultimate responsibility for ensuring that privacy is managed across the Council.
- 3.2.2 Directors and Branch Managers are responsible for ensuring development and implementation of departmental procedures consistent with Council's legislative obligations and this Policy.
- 3.2.3 The Governance Manager is responsible for monitoring and reporting to the Chief Executive Officer on the corporate implementation of Council's Privacy Policy.
- 3.2.4 The Organisation Development Manager is responsible for ensuring the delivery of privacy compliance induction to new staff and biennial staff refresher training through the corporate training and online learning management programs.
- 3.2.5 Each manager and supervisor is accountable for ensuring the implementation of the Privacy Policy through appropriate actions in their area of responsibility including ensuring all personal information is collected, used, stored, disclosed and disposed in accordance with the Council's Privacy and Records Management Policies.
- 3.2.6 Council staff will respect service users/client's right to privacy and confidentiality by ensuring the responsible use of the information obtained in the course of delivering Council services and that personal information about individuals is not made available to any person who does not have a legal right to this information.

3.3 Charter of Human Rights Compliance

It is considered that this Policy does not impact negatively on any rights identified in the Charter of Human Rights Act (2006).

PRIVACY POLICY

3.4 References

| | |
|--|---|
| Acts | Local Government Act 2020 (Vic.) Privacy and Data Protection Act 2014 (Vic.) Health Records Act 2001 (Vic.) Freedom of Information Act 1982 (Vic.) Public Records Act 1973 (Vic.) |
| Council Related Policies/Procedures | Information Management/Records Management Policy/Procedures Freedom of Information application process News and Social Media Policy Councillor & Staff Interaction Protocol (Responding to Councillor Information Request) |
| External | Office of the Vic. Information Commissioner – Guidance for the Victorian public sector: Drafting Privacy Policy |