# Privacy Policy

| | |
|---|---|
| **Title** | **Privacy Policy** |
| **Description** | A policy to ensure compliance with the Privacy and Data Protection Act 2014 and the Health Records Act 2001 |
| **Category** | Governance |
| **Type** | Policy |
| **Approval authority** | General Manager Governance, Communications and Customer Service |
| **Responsible officer** | Manager Governance and Integrity |
| **Approval date** | October 2023 |
| **Review cycle** | Every four years |
| **Review date** | October 2027 |
| **Document Reference (CM)** | D15/41842 |
| **Human Rights compatibility** | This policy has been assessed and is compatible with the Victorian Charter of Human Rights and Responsibilities |

## 1. Purpose

To articulate Council's policy in relation to compliance with the principles contained in the Privacy and Data Protection Act 2014 and the Health Records Act 2001.

## 2. Scope

This policy applies to officers and councillors of Yarra City Council, including Council contractors, consultants and volunteers.

Council believes that the responsible handling of personal and health information is a key aspect of good governance and is strongly committed to protecting an individual's right to privacy. Accordingly, Council is committed to full compliance with its obligations under the Privacy and Data Protection Act and Health Records Act.

## 3. Definitions

**Health Information** means -

(a) information or an opinion about—

(i) the physical, mental or psychological health (at any time) of an individual; or

(ii) a disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to him or her; or

(iv) a health service provided, or to be provided, to an individual - that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

**Personal Information** means -

(a) 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.

**Sensitive Information** means –

(a) information or an opinion about an individual's—

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record -

that is also personal information.

## 4. Policy

The Information Privacy Principles (IPP's) and Health Privacy Principles (HPP's) set out the minimum standards for how personal and health information should be managed in the Victorian public sector.

As part of our commitment to meeting the requirements of the Acts and demonstrating good governance, a description of Council's approach to each of the respective Information and Health Privacy Principles is outlined in the following section of this document.

Guidelines to the IPPs as outlined by the Office of Victorian Information Commissioner (OVIC) can be found on the OVIC website.

### *4.1. Collection (Principle 1)*

Personal or health information will only be collected where it is necessary to carry out Council functions and activities.

In some circumstances, collection of personal information is required by law.

Sensitive information is only collected where the individual has consented or as otherwise permitted under legislation.

If we collect information about an individual from another party, we will take reasonable steps to make them aware of this.

*Examples of information that may be collected include: Full Name, Address, Date of Birth, Signature, Email Address, Phone Number, Emergency Contact Details and Photo Identification.*

*Methods of information collection may include (and are not limited to) digital and hard copy forms and surveys submitted, social media, phone calls, emails and in-person contact.*

### *4.2. Use and Disclosure (Principle 2)*

Council will only use or disclose health and personal information for the primary purpose that it was collected, where the individual consents and for other related purposes that an individual would reasonably expect this to occur.

We may share relevant information when it is related to the reason the information was collected, with other work areas within Council, with external service providers and contractors (who are also bound by the same obligations) that have been engaged to provide the service or function on behalf of Council.

We will use and disclose information in circumstances where required by law and to protect the health, safety, or welfare of an individual or the public.

*For example, we may disclose personal information when reporting a matter to police or when members of the public access registers that Councils are required by law to make public.*

### *4.3. Data Quality (Principle 3)*

Council will ensure that the health and personal information it collects, uses, holds or discloses is accurate, complete, up to date and relevant to is functions or activities.

### *4.4. Data Security and Data Retention (Principle 4)*

Council will endeavour to maintain a secure system for storing personal and health information and will take reasonable steps to destroy or permanently de-identify information if it is no longer needed.

Information systems and operational policies and procedures are in place to protect health and personal information from misuse, loss, unauthorised access, modification or disclosure.

*For example, unsolicited personal information received will usually be destroyed or de-identified as soon as practicable.*

Council also has a program for the cyclical review of information collection and disclosure.

### *4.5. Openness (Principle 5)*

Council will ensure the most up-to-date version of this policy is made available on Council's website, Council's Intranet and will provide a copy to any person who requests it.

### *4.6. Access and Correction (Principle 6)*

Individuals have the right to access their own personal information and can request that we amend or delete incorrect or misleading personal information. Anyone can request access to documents held by Council however there are some exemptions under the Act.

*Examples of exemptions include:*

*• documents affecting personal privacy of other people (such as names, addresses,*

*telephone numbers) - section 33(1)*

*• documents relating to commercial information (putting a commercial business at an*

*unreasonable disadvantage) - section 34(1)*

*• information provided in confidence such as complaints – section 35(1)*

*• documents affecting legal proceedings (legal advice or opinions) - section 32(1)*

Access will be provided when requested except in circumstances outlined in legislation or where the Freedom of Information Act 1982 (Vic) applies.

Freedom of Information (FOI) gives a general right to individuals to access information held by Government agencies limited by exemptions.

All requests for access and correction should be made to the Privacy Officer (Manager Governance and Integrity) on 9205 5555.

Individuals are encouraged to contact the relevant Council area or the FOI Officer to determine whether information can be accessed before making a formal FOI request.

For details on how to make an application under the FOI Act, please refer to Council's website.

### *4.7. Unique Identifiers (Principle 7)*

Council will not assign, adopt, use, disclose or require unique health or other identifiers for individuals unless it is reasonably necessary to carry out its functions efficiently or if allowed or required by law.

*Examples of unique identifiers belonging to other organisations include Tax File Numbers, Medicare numbers, drivers licence numbers.*

### *4.8. Anonymity (Principle 8)*

Where lawful and practicable, Council will give you the option of not identifying yourself when supplying information or entering into transactions with Council. However, individuals need to be aware that anonymity may prevent us from taking appropriate action, resolving an issue or providing a response to the individual.

### *4.9. Transborder Data Flows (Principle 9)*

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

### *4.10A Sensitive Information (IPP 10)*

We will only collect sensitive information when an individual has consented, if collection is required or permitted by law, or when necessary for research or statistical purposes as permitted under the Privacy and Data Protection Act.

### *4.10B Closure Of The Practice Of A Health Service Provider (HPP 10)*

Health Information relating to a discontinued Council Health Service will be managed in accordance with the Health Records Act.

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

Where Council acts as a health service provider, it will make health information relating to an individual available to another health service provider if requested to do so by an individual and in accordance with the Health Records Act.

## 5. Provision of Services by External Parties

While personal and health information is usually handled by Council staff, Council may outsource some of its functions to third parties. This may require the service provider to collect, use or disclose certain personal or health information. Service providers are contractually obliged to comply with the requirements of either the Privacy and Data Protection Act or Health Records Act respectively.

## 6. Change Management

When altering systems or processes that collect, store or transfer private information, Council staff are to have regard to the implications of the change on Council's compliance with this policy.

Depending on the extent of the change, staff may consider one or more of the following supporting steps:

- engaging with relevant internal stakeholders as part of the change management process (e.g. the Privacy Officer for altering processes involving private information, Access Yarra staff for changes to front line information management practices, and Information Services for related information system changes).
- ensuring Information Services staff are involved in the procurement of new systems or upgrades to existing systems.
- implementing training and operating procedures to support staff in implementing any changes to processes and procedures.

Where significant changes are being considered, staff should undertake a formal Privacy Impact Assessment, using the tools produced by OVIC. These resources include a template for a Privacy Impact Assessment and are available on the OVIC website.

## 7. Complaints

If you feel aggrieved by Council's handling of your personal or health information, we encourage you to raise your complaint with Council's Privacy Officer on 9205 5555.

Your complaint will be investigated as soon as possible and you will be provided with a written response.

If you are not satisfied with how Council dealt with your complaint, you may make a complaint to OVIC or the Victorian Health Services Commissioner. It should be noted that the respective Commissioner may decline to hear the complaint if you have not first made a complaint to Council.

## 8. Breaches

Upon becoming aware of a breach or potential breach of the IPPs or HPPs, Council staff are to notify their direct supervisor without delay. Upon confirming that a breach has occurred, the direct supervisor shall notify both the relevant manager and Council's Privacy Officer.

Council's Privacy Officer shall refer to City of Yarra's information services incident response plan and be guided by advice provided by the Victorian Information Commissioner.

This advice requires the completion of the following steps:

(1) **Contain** the breach immediately to prevent any further compromise of personal information;

(2) **Assess** the risks of harm to affected individuals by investigating the circumstances of the breach;

(3) **Notify** affected individuals if deemed appropriate in the circumstances;

(4) **Review** the breach and the organisation's response to consider longer-term action to prevent future incidents of a similar nature and improve the organisation's handling of future breaches

## 9. Related Documents

- Privacy and Data Protection Act 2014
- Health Records Act 2001
- Local Government Act 1989
- Local Government Act 2020
- Freedom of Information Act 1982