



## INFORMATION PRIVACY POLICY

Responsible Officer: <b>Manager People and Governance</b>	Adoption Date:	17 April 2018
	Approved By:	Council
Authorising Officer: <b>Director Corporate Services</b>	Review Date:	June 2022
	Policy Type	Major Council Policy

### PURPOSE

The purpose of this policy is to ensure that personal and sensitive information collected by Council is handled in accordance with the requirements of the Information Privacy Principles contained in the *Privacy and Data Protection Act 2014 (Vic)* (the Act).

This Policy is administered by the Manager People and Governance.

### STATEMENT

Council must comply with the Act, the *Health Records Act (Vic) 2001*, and in relation to personal information, the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*. The main purposes of the Acts are:

- To establish a regime for the responsible collection, storage, handling and disclosure of personal and sensitive information.
- To provide individuals with rights of access to information about themselves which is held by the organisation.
- To provide individuals with the right to request an organisation to correct and amend information about themselves held by the organisation, including information held by contracted service providers.
- To require notification if there is unauthorised access to, or disclosure of, personal information which is likely to cause serious harm to an individual(s).

Council must conform to the ten privacy principles contained in the Act:

Principle 1 – Collection

Principle 2 – Use and Disclosure

Principle 3 – Data Quality

Principle 4 – Data Security

Principle 5 – Openness

Principle 6 – Access and Correction

Principle 7 – Unique Identifiers

Principle 8 – Anonymity

Principle 9 – Transborder Data Flows

Principle 10 – Sensitive Information

### **PRINCIPLE 1 COLLECTION**

Council must only collect personal information that is necessary for specific and legitimate functions and activities. This information will be collected by fair and lawful means and not in an unreasonably intrusive way.

Council will provide details of:

- Why it is collecting the information;
- How the information can be accessed;
- The purpose for which the information is collected;
- With whom the Council shares this information;
- Any relevant laws; and
- The consequences for the individual if all or part of the information is not collected.

Under normal circumstances Council must collect personal information about an individual only from that individual. However, if Council collects personal information about an individual from someone else, Council must take all reasonable steps to ensure that the individual is informed of his or her rights relating to the information collected.

### **PRINCIPLE 2 USE AND DISCLOSURE**

Council must not use or disclose personal information for a purpose other than the primary purpose except for those conditions specified in the Act including, but not limited to:

- Consent being given by the individual;
- Necessary to prevent a serious and imminent threat to an individual's life;
- Providing information to a law enforcement agency.

### **PRINCIPLE 3 DATA QUALITY**

Council must take reasonable steps to make sure that the personal information it collects, uses or discloses, is accurate, complete and as up-to-date as practicable for the nature and type of information being collected. E.g. the information needs to be up-to-date while it is being actively used for the primary purpose of collection.

### **PRINCIPLE 4 DATA SECURITY**

Council must take reasonable steps to protect all personal information it holds from misuse, loss, unauthorised access, modification or disclosure.

Where it is suspected that personal information has been misused, lost, accessed without authorisation, modified or disclosed, or where there has been an attempt to do so, and where it is likely to cause serious harm, Council must notify this data breach to the Australian Information Commissioner. Notification may only occur in accordance with the Unauthorised Access to, or Disclosure of, Personal Information Procedure.

Council must take reasonable steps to lawfully and responsibly destroy or permanently de-identify personal information when it is no longer required for the primary purpose or other directly related purposes.

### **PRINCIPLE 5 OPENNESS**

Council must make publicly available its policies relating to the management of personal information.

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

#### **PRINCIPLE 6 ACCESS AND CORRECTION**

Council must provide access to information held by Council about an individual on request except in specific circumstances as outlined in the Act including, but not limited to:

- The request for access is frivolous or vexatious;
- Denying access is required or authorised under law.

Where Council holds personal information about an individual and the individual is able to establish that information is incorrect, Council shall take reasonable steps to correct the information as soon as practicable but within 45 days of the request. If, however, Council denies access or correction, Council shall provide reasons for such determination.

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

#### **PRINCIPLE 7 UNIQUE IDENTIFIERS**

Council must not assign, adopt, use, disclose or require unique identifiers from individuals except for the course of conducting normal Council business or if required by law. Council will only use or disclose unique identifiers assigned to individuals by other organisations if the individual consents to the use and disclosure or the conditions for use and disclosure set out in the Act are satisfied

#### **PRINCIPLE 8 ANONYMITY**

Council must, where it is lawful and practicable, give individuals the option of not identifying themselves when entering into transactions with Council. E.g. Individuals may not wish to state their name when making complaints through Customer Services. It is imperative that Council's software systems have adequate flexibility to allow identification fields such as name to be left blank when appropriate.

#### **PRINCIPLE 9 TRANSBORDER DATA FLOWS**

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

#### **PRINCIPLE 10 SENSITIVE INFORMATION**

Council must not collect sensitive information about an individual except for circumstances as outlined in the Act. Reasons include, but are not limited to:

- Consent being given by the individual;
- The collection is required under law.

#### **BUSINESS USAGE**

Personal information about an individual held by Council may be used to carry out any of its internal functions efficiently where the use of information is related to the primary purpose of collection, or would reasonably be expected by the individual to be used for the purpose. E.g. rating and ownership information shared between departments.

This policy applies to all information collected by the Council and all employees of the Council.

## DEFINITIONS

**Personal Information** means 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 Schedule 2 of the Information Privacy Act 2000 applies.

**Primary Purpose** the initial reason that the information was collected. The reasons explained to the provider of information.

**Sensitive Information** means information or an opinion about an individuals

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

**Unreasonably intrusive.** Collecting personal information would be regarded as intrusive if it involves:

- Asking questions about sensitive personal affairs
- Physical touching, observing personal movements or invading private property
- Repeatedly and unnecessarily asking for the same personal information

**Unique Identifiers** means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name. E.g. tax file number.

**Health Information** is:

- 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 contained in a class of documents, that is prescribed as exempt health information for the purposes of the Health Records Act generally or for the purposes of specified provisions of that Act.

## RELATED PROCEDURES

*Unauthorised Access to, or Disclosure of, Personal Information Procedure.*

## REFERENCES

*Electronic Transactions (Victoria) Act 2000*  
*FairWork Act 2009 (Cth)*  
*Freedom of Information Act 1982 (Vic)*  
*Health Records Act 2001 (Vic)*  
*Local Government Act 1989 (Vic)*  
*Magistrates' Court Act 1989 (Vic)*  
*Occupational Health and Safety Act 2004 (Vic)*  
*Ombudsman Act 1973 (Vic)*  
*Privacy Act 1988 (Cth)*  
*Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*  
*Privacy and Data Protection Act 2014 (Vic)*  
*Public Records Act 1973 (Vic)*  
*Unclaimed Money Act 2008 (Vic)*  
*Victorian and Civil Administrative Tribunal Act 1998*