Privacy and Data Protection Policy

Council and your Privacy

Council collects and uses personal information to provide you with the services you require and is committed to the responsible handling of personal information in accordance with this Policy.

Policy statement

Council will ensure that it complies with the Information Privacy Principles (IPP's) contained in the *Privacy and Data Protection Act 2014* and the Health Privacy Principles (HPP's) in the *Health Records Act 2001* (the Acts).

Obligations under these Acts apply to Administrators, Councillors, Council staff (employees), agents (consultants, agency staff and volunteers) and contracted service providers.

This document outlines the objectives of the Policy, defines key privacy terms which are referenced in the Policy and sets out a process for handling privacy breaches and complaints.

Objectives

The Privacy and Data Protection Policy aims to:

- provide a regime for the responsible collection, storage, handling and disclosure of personal and health information;
- provide individuals with rights of access to personal and health information about themselves which is held by Council;
- provide individuals with the right to request Council to correct and amend information about them held by Council; and
- provide remedies for interferences with the information privacy of an individual;
- provide an accessible framework for the resolution of complaints regarding the handling of personal and health information.

Definitions

Key Terms	Definitions
Administrators	means persons appointed by the Minister for Local Government who constitute the Council and, subject to any conditions of appointment, perform the functions, powers and duties of Council.
Council	means the Whittlesea City Council
Councillors	means the elected members of Council

The Acts	means the *Privacy and Data Protection Act 2014* ('PDP Act') and *Health Records Act 2001* ('HR Act')
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 (excluding health information). Personal information held by Council may include your: • Name (current and former) • Address and/or email address (current and former) • Telephone number/mobile phone number • Date of birth • Occupation and annual salary • Medicare number • Credit card and bank account numbers • Details of any Council services used by you. Council may also request personal information to provide education, health and other community services such as immunisation services, kindergarten services, maternal and child health and school holiday programs. In some instances, personal information may be contained on a public register. For example, register of building permits, food premises and animal registration details.
Health Information	includes personal information or opinion about: • An individuals' physical, mental or psychological health • An individual's disability • Preferences about future provision of health services to them • Health services provided, or to be provided, to an individual For example, Council holds health information on clients who use home and community care services or family day care services.
Sensitive Information	means a type of personal information which includes an individual's racial or ethnic origin or heritage, political views, religious beliefs, sexual preferences and membership of groups or criminal record.
Third Party	in relation to personal information, means an individual or body other than the organisation holding the information and the individual to whom the information relates.
Primary Purpose	means the main reason/s the personal information was shared with or collected by Council.
Reasonable Secondary Purpose	must be related to the primary purpose of collection and be consistent with what an individual would reasonably expect. In

	the case of sensitive information, the secondary purpose must be directly related. Would the individual whose information was collected reasonably expect the use or disclosure? For example, Council collects information from ratepayers in relation to property ownership. The primary purpose of collection relates to levying rates and charges, however, disclosure of this information to emergency authorities for the secondary purpose of public safety against bushfire, flood or extreme weather would be a related and reasonably expected secondary purpose.
HPP's	means the following Health Privacy Principles (HPP's) contained in the *Health Records Act 2001*: 1. Collection 2. Use and Disclosure 3. Data Quality 4. Data Security& Data Retention 5. Openness 6. Access and Correction 7. Identifiers 8. Anonymity 9. Transborder Data Flows 10. Transfer or Closure of the Practice of a Health Service Provider 11. Making Information Available to Another Health Provider
IPP's	means the following Information Privacy Principles contained in the *Privacy and Data Protection Act 2014*, as follows: 1. Collection 2. Use and Disclosure 3. Data Quality 4. Data Security 5. Openness 6. Access and Correction 7. Unique Identifiers 8. Anonymity 9. Transborder Data Flows 10. Sensitive Information
Privacy Impact Statement	is an assessment of any actual or potential effects that the activity or proposal may have on individual's privacy and the ways in which any adverse effects may be mitigated.
Public Registers	hold documents that are open to inspection by members of the public and contain information required or permitted by legislation.

	For example, register of building permits, food premises and animal registration details.
Contracted Service Provider	is a service provider which is required to comply with the Acts due to entering into a contract with Council.
Agent	means an individual or organisation employed by Council to perform a service that involves handling personal information. An agency relationship means that Council will usually be held responsible for how their agents (like their employees) handle personal information.
Document	may be in writing, electronic or paper format and may refer to books, scans, photographs, emails and documents stored in a physical file, database or spread sheet.
Social media	is a broad term that refers to the various activities that integrate technology, social interaction and the construction of words, pictures, video, and audio. For example, blogs, instant messaging, podcasts, forums and postings.

Context/Rationale

Council must set out in a document a clearly expressed policy on its management of personal information and make this document available to anyone who asks for it.

The policy ensures Council complies with its obligations under the *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001 (Vic)* and demonstrates Council's openness and commitment to good governance.

Scope

The policy applies to Administrators and Councillors, employees, contractors and volunteers of Council.

The policy covers personal information held by Council and includes personal information Council has collected about individuals including:

- information collected on Council forms, in person, in correspondence, over the telephone or via our website; or
- from a third party such as agents and contracted service providers.

Key linkages

All Council policies comply with the *Victorian Charter of Human Rights and Responsibilities*.

This policy has clear linkages to:

- *Privacy and Data Protection Act 2014* (Vic)
- *Health Records Act 2001 (Vic)*
- OVIC Guidelines on the Information Privacy Principles (2019)
- OVIC Report investigating Local Government privacy policies (2019)
- City of Whittlesea Information Technology Systems, Access and Use Policy

You can request to access your personal information

Council will provide access to information held by Council about an individual to that individual on request, except in specific circumstances as outlined within the PDP Act.

Requests for access to and correction of documents containing personal information are generally managed under the *Freedom of Information (FOI) Act 1982*. FOI requests must be made in writing and are accompanied by an application fee. Please see Council's website for more information regarding how to make an application or contact a Freedom of Information Officer on 9217 2294.

Some requests for personal information may be dealt with informally (outside of the FOI Act). Please contact Council's Privacy Officer on 9217 2223 to discuss your requirements.

Where Council holds personal information about an individual and the individual believes that information is incorrect, Council will take reasonable steps to correct the information as soon as practicable and within 30 days of the request. If Council denies access or correction, Council will provide reasons.

If Council and an individual disagree about the accuracy of personal information held by Council, Council will take reasonable steps to record a statement relating to the disputed information if requested by the individual.

If you are not satisfied with Council's resolution of an information privacy matter you may make a complaint to the Office of the Victorian Information Commissioner (OVIC) Post: PO Box 24274, Melbourne Vic 3001 or Email: enquiries@ovic.vic.gov.au.

Responding to a privacy complaint

The following complaint process is available for person who feels aggrieved by Council's handling of their personal information or believes that a Council officer is in breach of the *Privacy and Data Protection Act 2014* or the *Health Records Act 2001.*

Complaint should be directed to Council's Information Privacy Officer.

Mail: Privacy Officer, City of Whittlesea, Locked Bag 1, MDC Bundoora, Vic 3083

Email: privacy@whittlesea.vic.gov.au

Telephone: 9217 2223

Definition of a formal complaint

- The complaint must be in writing (email is acceptable). If making a complaint in writing unreasonably disadvantages you, you may request to make the complaint in another form that enables you to do so such as verbally;
- The complainant must provide a brief description of the incident, for example; date of the incident, what personal information was involved (name, address, financial, medical) and what form it was in (paper records, electronic, etc);
- The complainant must be the person who is directly involved in the complaint or their authorised representative; and

- The complainant may withdraw a complaint at any time. A request for a withdrawal of a complaint must be referred to the Information Privacy Officer.

When a complaint is received that is deemed to be a formal complaint, the Council's Information Privacy Officer will be assigned to handle the complaint as the investigating officer.

Alternatively, a complaint may be made to the Office of the Victorian Information Commissioner. The Commissioner may decline to hear the complaint if Council has not had the opportunity to consider the complaint first.

Responding to a privacy breach

All privacy complaints and breaches will be referred to Council's Information Privacy Officer on 9217 2223 or email privacy@whittlesea.vic.gov.au

A privacy breach occurs when personal, sensitive or health information of an individual is misused, lost or subjected to unauthorised access, modification or disclosure by Council.

Council's Privacy Breach Procedure sets out the process to be followed by Council staff if a privacy breach occurs or staff suspect that a privacy breach has occurred.

Privacy Breach Procedure

This procedure involves a four-step process in responding to a privacy breach:

Step 1 Contain the breach and make a preliminary assessment;

Step 2 Evaluate the risks for individuals associated with the breach;

Step 3 Consider breach notification to affected individuals and others (not all breaches warrant notification). Is there a risk of serious harm? Risk assessment to be undertaken on a case by case basis;

Step 4 Review the incident and take action to prevent future breaches; fully investigate the cause of the breach and implement prevention strategies and a prevention action plan.

Administration

Council's Governance Advisor is the Information Privacy Officer ('the IPO'). The IPO has the responsibility to assist Council to comply with its obligations under the Acts.

The IPO is authorised to provide advice on the Acts and to receive privacy complaints and requests for access and correction of personal information.

The IPO is responsible for reviewing the Privacy and Data Protection Policy and any Procedural Guidelines. The IPO is also responsible for promoting the Policy to staff and, when necessary, liaising with management to ensure compliance with the Acts.

The IPO is also responsible for co-ordinating privacy training for staff and promoting staff awareness of the IPP's.

Review

The Privacy and Data Protection Policy will be reviewed regularly to consider changes in relevant legislation or guidelines or as required by the Executive Leadership Team.

This Policy will be reviewed no later than 30 June 2022.