



Information Privacy Policy

Contents

1	Document Control	1
2	Purpose.....	2
3	Scope.....	2
4	Policy details	2
4.1	Collection (Principle 1)	2
4.2	Use and Disclosure (Principle 2)	3
4.3	Data Quality (Principle 3).....	3
4.4	Data Security and Retention (Principle 4).....	3
4.5	Openness (Principle 5).....	3
4.6	Access and Correction (Principle 6)	4
4.7	Unique Identifiers (Principle 7).....	4
4.8	Anonymity (Principle 8)	4
4.9	Transborder Data Flows (Principle 9).....	4
4.10	Sensitive Information (Principle 10).....	4
4.10.1	Transfer or Closure of Health Service (Health Privacy Principle 10).....	5
4.11	Making Health Information available to another provider (Health Privacy Principle 11).....	5
5	Privacy Breaches	5
6	Responsibility	6
7	Related Documents and Resources	6

1 Document Control

The electronic version of this document is the controlled version. Printed copies are considered uncontrolled. Before using a printed copy, verify that it is the current version.

RESPONSIBLE GENERAL MANAGER	General Manager Corporate Services
DOCUMENT OWNER	Manager Governance
APPROVED/ADOPTED BY	Chief Executive Officer on 19 August 2020
SIGNATURE	
APPROVAL DATE (In addition state effective if different)	19 August 2020
REVIEW DATE	19 August 2023
CM REF AND VERSION	09/28466 [v6]

VERSION HISTORY	<p>This Policy Replaces Version 4</p> <p>Version 4 – CEO approved 12 May 2019</p> <p>Version 3 – CEO approved 15 May 2012</p> <p>Version 2 – Council approved 30 April 2007</p> <p>Version 1 – Council approved 24 June 2002</p>
-----------------	--

2 Purpose

Council’s Information Privacy Policy illustrates the ways in which we comply with principles and legislative requirements under the Privacy and Data Protection Act 2014 (PDP) and Health Records Act 2001. A clear and accurate privacy policy supports a positive, trusting relationship between Council and members of the public and highlights council’s commitment to always conduct business in accordance with the cornerstones of our Good Governance Framework: leadership and direction, transparency, integrity and accountability. The ongoing development and review of our privacy policy is part of Council’s privacy governance and commitment to best practice.

3 Scope

The Policy relates to all personal and health information about an individual that is collected, stored, used or disclosed by Council and applies to all people working within Council including Councillors, contractors and volunteers. The policy is promoted by Council’s Privacy and Data Protection Committee that builds capability and confidence for good judgement and decision making across the organisation.

4 Policy details

The Information and Health Privacy Principles 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, we have outlined our approach in complying with each of the overarching Information and Health Privacy Principles as follows.

4.1 Collection (Principle 1)

Personal or health information will only be collected where it is necessary to carry out our functions and activities. In some circumstances, collection of personal information is required by law. Sensitive information such as details pertaining to date of birth 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.

At or near the time of collection, we will notify the individual of the purpose of collecting the information and inform the individual how they can access the information. Collection Notices, such as the example below, are included on every form and explain how we intend to use, share and disclose any personal information collected.

The City of Kingston is committed to protecting your privacy. The personal information requested on this form is being collected by City of Kingston 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 receiving the personal information] for the purpose of [insert how the entities will use 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, please contact City of Kingston via telephone [insert number for your work area] or email [insert email address for your work area].

4.2 Use and Disclosure (Principle 2)

We 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.

For example:

- a. *Council may use email addresses or mobile phone numbers to inform residents that could be significantly affected, of unplanned events*
- b. *Council would NOT utilise email addresses or mobile phone numbers to advertise an event or for other marketing purposes*

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.

Personal information is also held in registers that are available for public inspection at the Council office.

Examples of personal information held by Council that is accessible by the public include:

- *Council lease of land information (from July 2021)*
- *Register of all registered dogs and cats*
- *Decisions and determinations relating to planning permits*
- *Register of Authorised officers*
- *Summary of personal interest returns*
- *Advertised and open tender information (via Tenderlink)*

4.3 Data Quality (Principle 3)

We will take reasonable steps to ensure that all personal and health information collected, held, used and disclosed is accurate, complete, up-to-date and relevant to Council's purpose, functions and activities. Information will be verified and updated at the time of collection.

For example, our staff will ask for personal details to verify your identity before actioning a request to update your postal address.

4.4 Data Security and Retention (Principle 4)

We maintain a secure system for storing personal and health information and take reasonable steps to destroy or permanently de-identify information when it is no longer needed. Information systems, operational policies, procedures and a Privacy and Data Protection Committee are in place to ensure compliance and to review, maintain and protect personal and health information from misuse, loss and from unauthorised modification or disclosure.

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

4.5 Openness (Principle 5)

We will take reasonable steps to let people know about the type of information we hold, the purpose for holding it, and how we collect, use and disclose that information. We have established procedures to respond to queries about our personal information handling practices and clearly expressed policies on the way we manage personal information.

Our Information Privacy Policy is published on our external website and is available to anyone who asks for 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.

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, refer to Council's website [here](#).

4.7 Unique Identifiers (Principle 7)

At times we may assign a code or number to someone's record to assist with identification. This can take the form of an employee number, client code, reference or invoice number. We only assign, use, disclose or require a unique identifier for the course of conducting business activities efficiently or as required by law.

For example, we utilise the invoice number on an account instead of using someone's name when paying an account

4.8 Anonymity (Principle 8)

Where lawful and practicable, we will give individuals the option of remaining anonymous when supplying information or entering into transactions with us. 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)

When transferring information outside of Victoria, we will take reasonable steps to ensure that the recipient of the information is bound by privacy protection requirements similar to the Victorian Information Privacy Principles.

4.10 Sensitive Information (Principle 10)

The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record.

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

4.10.1 Transfer or Closure of Health Service (Health Privacy Principle 10)

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

4.11 Making Health Information available to another provider (Health Privacy Principle 11)

If an individual asks us to make their health information available to another service provider, we will comply with the request as soon as practicable. Our Health Services will provide information to other health providers in accordance with the Health Records Act.

5 Privacy Breaches

A data breach occurs when personal information held by an organisation is subject to misuse or loss or to unauthorised access, modification or disclosure.

A data breach can be accidental or as a result of a malicious act from an external or internal party.

Examples of data breaches include:

- *An employee takes paper records, an unencrypted USB stick or laptop out of the office and the information is lost or stolen*
- *An organisation mistakenly provides personal information to the wrong person*
- *An email containing recipients' email addresses is forwarded to unintended parties*
- *An organisation's database is illegally accessed by staff members or by individuals outside of the organisation*

We will act quickly to investigate and understand any privacy breach incidents and take appropriate steps to manage any potential consequences for affected individuals.

Your right to make a privacy complaint

If you have concerns about how Council has handled your personal information, you have the right to make a complaint. If you believe that we have breached your privacy rights, you should first make a complaint to Council's Privacy Officer and try to resolve the issue.

If you aren't satisfied with the way Council dealt with your concerns, you can make a complaint to the Office of the Victorian Information Commissioner (OVIC).

Email Council:
info@kingston.vic.gov.au;

Post:
PO BOX 1000
Mentone VIC 3194

Complaints to Council should be made in writing. The complaint will be investigated by Council's Information Privacy Officer and the complainant will be provided with a written response within 10 working days.

6 Responsibility

It is the responsibility of the Governance team to review this Policy every three years and in accordance with relevant legislation.

7 Related Documents and Resources

Legislation / External Document

- Privacy and Data Protection Act 2014
- Freedom of Information Act 1982
- Health Records Act 2001
- Charter of Human Rights and Responsibilities Act 2006
- Local Government Act 2020

Internal Documents

- Media and External Communications Policy
- Social Media Policy
- Public Transparency Policy
- CCTV Code of Practice
- Code of Conduct

A copy of this Privacy Policy is available to all staff via Council's intranet and Council's external website. City of Kingston websites.

The following applies when you interact with our websites.

Collection and use of personal data

The City of Kingston's various websites only collect or record personal information you choose to provide through our Contact Us section, subscription to communications, newsletters, initiatives or program updates, online applications etc. You can browse our websites anonymously, without disclosing your personal information.

Collection and use of site visit data

Cookies are data files that are placed on a device when it is used to visit a website. For the most part they are sessional and just contain system-generated values to identify the user's session for statistical and system administration purposes only. Cookies are used on our sites, but they do not collect any personal information.