

# Information Privacy Policy



City of  
**KINGSTON**

## Contents

1. Purpose of the Policy .....	2
2. Scope .....	2
3. Definitions .....	2
4. Responsible Executive .....	3
5. Policy Owner .....	3
6. Related Documents .....	3
7. Delegation Authority .....	3
8. Policy Statement .....	3
9. Policy Details .....	3
9.1 Roles and Responsibilities .....	3
9.2 Privacy Statements .....	5
9.3 Privacy Principles .....	5
Appendix II - Information Privacy Principles .....	9
Appendix II - Health Privacy Principles .....	10

APPROVAL / VERSION NO:	Version 1 - Council approved 24 June 2002 Version 2 - Council approved 30 April 2007 Version 3 - CEO approved 15 May 2012 Version 4 - CEO approved 12 May 2015
TRIM REF:	09/28466
REVIEW	Next review due May 2017
RESPONSIBLE EXECUTIVE	General Manager Corporate Services
POLICY OWNER	Manager Information Services

## 1. Purpose of the Policy

To meet the information privacy principles (IPPs) and health privacy principles (HPPs) set out in the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) in relation to the management and handling of personal and health information within the public sector.

## 2. Scope

This Policy applies to all employees, Councillors, contractors, and volunteers of the City of Kingston.

This Policy covers all personal and health information held by the City of Kingston, that is, information, or an opinion about an individual, whose identity is apparent, or can be reasonably ascertained, from that information or opinion. This includes information we have collected in any format including correspondence, in person, over the phone, and over the Internet.

Council's privacy policies will require approval by the Chief Executive Officer.

## 3. Definitions

**Personal Information** – means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years.

**Health Information** – means information or an opinion about the physical, mental, or psychological health of an individual, a disability of an individual, the individual's expressed wishes for the future provision of health services to them, or a health service provided or to be provided to an individual. It also includes other personal information collected to provide, or in providing, a health service.

**IPPs** – Information Privacy Principles. Set of principles that regulate the handling of personal information.

**HPPs** – Health Privacy Principles. Set of principles that regulate the handling of health information.

**Sensitive Information** - personal information or an opinion about an individual's:

- Race 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 trade association; or
- Membership of a trade union; or
- Sexual preferences or practice; or
- Criminal record.

**Social Media** – is an umbrella term that defines 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.

#### 4. Responsible Executive

General Manager Corporate Services.

#### 5. Policy Owner

Manager Information Services.

#### 6. Related Documents

Victorian Privacy and Data Protection Act 2014.

Victorian Health Records Act 2001.

Social Media Policy (10/104456).

Privacy Statement – Generic (06/32350).

Privacy Statement – Competitions and Offers (07/45126)

Photo Permission Form – (11/24798).

#### 7. Delegation Authority

There is no formal delegation relevant to this Policy.

#### 8. Policy Statement

The Council has obligations:

- under the Privacy and Data Protection Act to collect and handle personal information according to the 10 IPPs; and
- under the Health Records Act to collect and handle health information according to the 11 HPPs.

#### 9. Policy Details

##### 9.1 Roles and Responsibilities

The Council's Chief Executive Officer is responsible for the appointment of the City of Kingston's Information Privacy Officer and Information Privacy Committee.

The role of the Information Privacy Officer:

- Inform and educate Council officers of their obligations under the Privacy and Data Protection and Health Records Acts and to handle difficult enquiries, complaints or adjustments concerning personal or health information.
- Provide advice and guidance to staff and the Privacy Committee members on privacy related matters and document for learning purposes and consistency.
- Maintain all documentation relating to the management and implementation of the Privacy and Data Protection and Health Records Acts for the City of Kingston.

- Apply normal photocopying or administrative charges for information requested at his/her discretion.
- Respond to requests for access to and correction of personal information in consultation with Council Officers in accordance with Council's customer service standards and this Information Privacy Policy.
- Investigate privacy complaints in consultation with complainants and Council Officers. Assess the facts of each alleged breach against the Information Privacy Principles and the Health Privacy Principles and make recommendations. Respond to complainants and conciliate where necessary. If the complainant is not satisfied with Council's response they may approach the Victorian Government's Privacy Commissioner and/or the Health Services Commissioner (as appropriate) for resolution. Team Leader Corporate Information is responsible for handling notice of complaints from the respective Privacy Commissioners in accordance with S7 Instrument of Sub-Delegation (14/60085).
- Keep a record of alleged breaches in Council's Privacy Complaints / Breaches Register (06/32238) and report findings and recommendations to the Privacy Committee.
- Respond to requests for access to and correction of health information in accordance with the Freedom of Information Act 1982 (Vic) and the Health Records Act.
- Provide updates to the Privacy Committee on legislative changes relating to information privacy.
- Ensure Council's privacy statements are accurate and up to date including privacy related information published on Council's websites (Internet/Intranet).
- Coordinate bi-annual Privacy Committee meetings including the preparation of agendas and minutes.

The role of the Privacy Committee:

- Meet bi-annually under the direction of the Privacy Committee chairperson.
- Member representation across various areas of Council including:
  - General Manager Corporate Services (Chairperson);
  - Privacy Officer (Minutes);
  - Team Leader Corporate Information;
  - Program Leader Governance;
  - Team Leader Customer Service; and
  - Other areas/roles as determined by the Privacy Committee.
- Review of the Information Privacy Policy every two years and seek approval of any changes by the Chief Executive Officer.
- Review proposed changes to existing or new privacy statements put forward by Council Officers / Departments.

- Consider privacy related matters raised by the Privacy Officer and other Committee members.
- Membership to the committee will be reviewed every two years in conjunction with the review of this policy. Team leaders and managers across Council are encouraged to become members of the committee.

## **9.2 Privacy Statements**

A general statement outlining Council's position on the handling of personal information will be used at all points of collection and all outgoing correspondence that may request personal or health information. This will include Kingston's website, advertising material, standard forms and correspondence requesting personal or health information.

Forms collecting information that is to be used for a specific purpose will include a privacy statement on the form including the purpose of collection.

Council's approved privacy statements will be published in the relevant publications (e.g. forms, websites), confirming Council's commitment to the personal information and health information privacy principles.

## **9.3 Privacy Principles**

The City of Kingston will manage personal information and health information as outlined in the following principles.

- **Collection of Information**

The City of Kingston will only collect personal information that is necessary for specific and legitimate functions of Council.

The City of Kingston will only collect health information that is necessary for specific and legitimate functions of Council, and following the additional collection requirements of the HPPs.

Information will be collected by fair and lawful means, and not in an unreasonably intrusive way.

Where reasonable and practicable to do so, Council will collect personal and health information directly from the individual involved. However, Council reserves the right to collect personal and health information from third parties where the law or circumstances warrant it.

In most cases, Council will advise individuals of its privacy practices, including the purposes for which their information is being collected, and of those third parties to whom their information is usually disclosed etc. However, Council reserves the right not to do so where permitted by law.

Sensitive information will only be collected where the individual has consented or collection is otherwise required or permitted by law.

Sensitive information will be treated with the utmost security and confidentiality and only used for the purpose for which it was collected.

Personal Information is also collected through social media. Employees who use social media at the City of Kingston are required to adhere to this Information Privacy Policy and the Social Media Policy.

- **Use and Disclosure of Information**

The City of Kingston will not use or disclose information about an individual other than for the primary purpose for which it was collected, unless one of the following applies:

For personal information - it is for a related purpose that the individual would reasonably expect;

For sensitive and health information - it is for a directly related purpose that the individual would reasonably expect;

Where Council has the consent of the individual to do so;

If, as defined in the Health Records Act, the individual is incapable of giving consent; or

As otherwise required or permitted by the Privacy and Data Protection and Health Records Acts or any other legislation.

- **Data Quality**

Council will take reasonable steps to ensure that all personal, sensitive and health information collected, held, used and disclosed is accurate, complete and up to date, bearing in mind and relevant to its purpose, functions and activities.

- **Data Security and Retention**

Council will take reasonable steps to prevent misuse or loss or unauthorised access, modification or disclosure of personal and health information.

Personal and health information will be managed confidentially and securely and destroyed, de-identified or archived in accordance with Public Record Office Victoria (PROV) standards.

Council will monitor and implement reasonable and appropriate technical advances or management processes, to provide an up to date ongoing safeguard for personal information.

- **Openness**

The City of Kingston Information Privacy Policy will be available on Kingston websites or on request at Customer Service Centres and Libraries.

- **Access to and Correction of Information**

Individuals have a right to request access to any personal or health information held about them, and may request any incorrect information be corrected.

Council may decide not to allow access to personal information or health information in accordance with the exemptions contained within the Privacy and Data Protection and Health Records Acts.

The process for requesting the correction of personal and health information, i.e. documents, is through a Freedom of Information application.

- **Unique Identifiers**

Council will not assign, adopt, use, disclose or require unique health or other identifiers from individuals except for the course of conducting normal business or if allowed or required by law.

- **Anonymity**

Council will, where it is lawful and practicable, give individuals the option of not identifying themselves when entering into transactions with Council.

Council will ensure that individuals are aware of all, if any, limitations to services if the information requested is not provided.

- **Transborder Data Flows**

The City of Kingston will only transfer personal or health information outside of Victoria in accordance with the provisions outlined in the Privacy and Data Protection and Health Records Acts.

- **Sensitive Information**

The City of Kingston will not collect sensitive information unless an individual has consented or collection is required or permitted by law, or when necessary for research or statistical purposes as permitted under the Privacy and Data Protection Act.

Personal Information is also evident and collected through social media. Council employees who use social media are required to adhere to the Social Media Policy which is accessible on Council's Intranet.

- **Transfer or Closure of Health Service**

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

- **Making Health Information available to another service provider**

Council's Health Services will provide health information to other health providers in accordance with the Health Records Act.

#### **10. Decision Guidelines**

There is no additional information for this Policy.

#### **11. Transition/Translation Arrangements**

Policy commenced in June 2002.

#### **12. Review**

Policy to be reviewed by May 2017.

## Appendix 1 - Information Privacy Principles

### IPP 1 - Collection

Collect only personal information that is necessary for the performance of functions, for a pre-determined purpose. Collect lawfully, fairly and not unreasonably intrusively. Advise individuals that they can gain access to their personal information.

### IPP2 - Use and Disclosure

Use and disclose personal information for the primary purpose for which it was collected, or a related purpose a person would reasonably expect; otherwise, use and disclosure can only occur with consent. There are exemptions to disclosure restrictions, e.g. law enforcement, life-threatening emergencies.

### IPP 3 – Data quality

Make sure personal information is accurate, complete, and up-to-date.

### IPP 4 – Data Security

Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. Personal information should be destroyed or de-identified when it is no longer needed. Destruction should be in accordance with disposal schedules of the *Public Records Act 1973*.

### IPP 5 - Openness

Document clearly expressed policies on the management of personal information and provide the policies to anyone who asks. Know where to find the policy. Know who your privacy contact person is. Make sure the policy is reviewed to reflect current practice.

### IPP 6 – Access and Correction

Individuals have a right to seek access to their personal information and make corrections. Most requests for access and correction are handled under the Victorian *Freedom of Information Act 1982*.

### IPP 7 – Unique identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purpose of an organisation's operations, e.g. tax file no., driver's license number. Unique identifiers can facilitate data matching, and this can in turn diminish privacy. So this IPP limits the assignment, adoption, and sharing of unique identifiers

### IPP 8 - Anonymity

Agencies must give individuals the option of not identifying themselves when entering transactions, if that is lawful and feasible.

### IPP 9 – Transborder data flows

Personal information can only be transferred interstate or overseas if certain conditions are met. Consent is one condition. Another condition is that the destination must have privacy standards similar to Victoria's IPPs.

### IPP 10 - Sensitive information

Collection of sensitive information is tightly restricted. This includes information or opinion about an individual's: political views; religious beliefs; sexual preferences; membership of groups (e.g. unions, political groups); racial or ethnic origin; or criminal record.

## Appendix II - Health Privacy Principles

### IPP 1 - Collection

Collect only personal information that is necessary for the performance of functions, for a pre-determined purpose. Collect lawfully, fairly and not unreasonably intrusively. Advise individuals that they can gain access to their personal information.

### IPP2 - Use and Disclosure

Use and disclose personal information for the primary purpose for which it was collected, or a related purpose a person would reasonably expect; otherwise, use and disclosure can only occur with consent. There are exemptions to disclosure restrictions, e.g. law enforcement, life-threatening emergencies.

### IPP 3 – Data quality

Make sure personal information is accurate, complete, and up-to-date.

### IPP 4 – Data Security and Data Retention

Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. Personal information should be destroyed or de-identified when it is no longer needed. Destruction should be in accordance with disposal schedules of the *Public Records Act 1973*.

### IPP 5 - Openness

Document clearly expressed policies on the management of personal information and provide the policies to anyone who asks. Know where to find the policy. Know who your privacy contact person is. Make sure the policy is reviewed to reflect current practice.

### IPP 6 – Access and Correction

Individuals have a right to seek access to their personal information and make corrections. Most requests for access and correction are handled under the Victorian *Freedom of Information Act 1982*.

### IPP 7 – Identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purpose of an organisation's operations, e.g. tax file no., driver's license number. Unique identifiers can facilitate data matching, and this can in turn diminish privacy. So this IPP limits the assignment, adoption, and sharing of unique identifiers

### IPP 8 - Anonymity

Agencies must give individuals the option of not identifying themselves when entering transactions, if that is lawful and feasible.

### IPP 9 – Transborder data flows

Personal information can only be transferred interstate or overseas if certain conditions are met. Consent is one condition. Another condition is that the destination must have privacy standards similar to Victoria's IPPs.

### IPP 10 - Transfer/closure practice

If the practice or business of a health provider is sold or transferred or if the provider is deceased, steps must be taken to notify individuals who have received health services from the provider.

### IPP 11 - Making information available to another service provider

An individual can request that a service provider make information relating to them available to another service provider.