
VISION

A place for people to prosper -
alive with opportunity

MISSION

Working together
Committed to our values
Serving our community

VALUES

INTEGRITY
RESPECT
INCLUSIVENESS
SERVICE



POLICY TITLE	City of Cambridge Privacy Policy
CATEGORY	Corporate
POLICY NUMBER	CRP-220.010
DEPARTMENT	Corporate Services
DIVISION	City Clerk
AUTHORITY	Departmental/Operational
APPROVED BY	Not Listed
EFFECTIVE DATE	June 23, 2014
REVIEW DATE	Not Listed

POLICY STATEMENT

Privacy plays a key role in a free, democratic society and is an essential element in maintaining public trust in government. The City of Cambridge is committed to protecting the privacy of individuals, and will ensure that privacy protection continues to play a key role in an open, accessible and transparent government.

PURPOSE

The purpose of this policy is to foster greater public trust by establishing clear accountability statements, including roles and responsibilities, for the protection of personal information collected, used, disclosed and disposed by the City of Cambridge.

DEFINITIONS

N/A

AUTHORITY

Clerk's Division

SCOPE

Employees, affiliated organizations, residents

VISION

A place for people to prosper -
alive with opportunity

MISSION

Working together
Committed to our values
Serving our community

VALUES

INTEGRITY
RESPECT
INCLUSIVENESS
SERVICE



POLICY

1. The City of Cambridge is committed to protecting the privacy of any recorded personal information gathered by the city. The practices of the City of Cambridge related to the gathering and handling of personal information are designed to comply with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act.
2. Whenever City of Cambridge staff members collect personal information, they will collect only the personal information that is needed to carry out the specific function for which the information is being gathered.
3. The City of Cambridge will not share any personal information with any other organization or individual unless authorized do so by statute or with the consent of the person to whom the information relates. Within the corporation personal information will be made available only to those staff members who need the information to respond to inquiries or to otherwise perform their job functions. The city will endeavour to put safeguards in place wherever personal information is handled.
4. Nor will this information be provided to a third party for data base production, except as permitted by statute or with the express permission of the person to whom the information relates.

Collection of Personal Information

5. Whenever personal information is collected, used or disclosed by city staff, it must be handled in accordance with the protection of privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act. This applies to all personal information in any format in any application.
6. Whenever the city enters into an agreement in which an external party is responsible for collecting or otherwise handling personal information on behalf of the city, staff will ensure, either through a separate data sharing agreement or specific wording in the body of the contract, that all agreements meet the city's obligations to protect that personal information as required by MFIPPA. At a minimum these agreements will note that the personal information remains subject to the requirements of MFIPPA at all times and will specifically address the collection, access, retention, use, disclosure, disposal, confidentiality and security of the personal information. A data sharing agreement is not required in situations where consultants might encounter personal information while performing work on city servers. A confidentiality agreement is sufficient in these cases.
7. City staff that collects personal information through the city web site, will ensure that the city's obligations concerning collection, access, retention, use, disclosure, disposal, confidentiality and security of personal information are met.
8. Compliance - Employees who fail to comply with this policy will be subject to the appropriate disciplinary action, up to and including termination of employment. Union employees will be disciplined subject to any applicable provisions of their particular collective agreement:

VISION

A place for people to prosper -
alive with opportunity

MISSION

Working together
Committed to our values
Serving our community

VALUES

INTEGRITY
RESPECT
INCLUSIVENESS
SERVICE



Offences include:

- wilfully disclosing personal information in contravention of MFIPPA;
- wilfully maintain a personal information bank that contravenes MFIPPA;
- alter, conceal or destroy a record, or cause any other person to do so, with the intention of denying a right under MFIPPA to access the record or the information contained in the record.

Privacy Complaints or Inquiries

9. Complaints or inquiries about the City's privacy policies and/or practices relating to the handling of personal information should be directed to the FOI Co-ordinator who will investigate. If a complaint is held to be justified, appropriate corrective measures will be taken, including amending this policy, as necessary.
10. Integrated Incident Management Privacy Policy for Community Services Department.
11. If an employee leaves their desk, the following must be done in order to prevent unauthorized access: logout from any databases or computer programs containing personal information or assessments related to clients.
12. Records shall be retained and disposed of in a fashion consistent with the City's existing policies and procedures.
13. Access to paper records shall be provided for the purposes of fulfilling a business requirement.
14. Storage facilities, retrieval and access procedures should ensure personal data are held securely and access provided on a controlled basis only. Security procedures should comply with the records management policy or accepted external standards.
15. No employee is permitted to destroy or alter documents without proper authority or provide inappropriate access to restricted documents.
16. When a compromising incident regarding a patient's assessment records is detected, the incident is to be reported to the HIC (Health Information Custodian) privacy officer.
17. The HIC privacy officer processes the reported/detected incident – containment is the first priority – and determines if the incident involves other participating organizations. The HIC either sends an Incident Report (Appendix A) to the HINP (Health Information Network Provider) if external parties are involved, or for internal disclosures refers to section 8 of this policy.



VISION

A place for people to prosper -
alive with opportunity

MISSION

Working together
Committed to our values
Serving our community

VALUES

INTEGRITY
RESPECT
INCLUSIVENESS
SERVICE



The HIC privacy officer documents the incident, initiating the internal processes, which would involve notification to the client regarding the privacy breach of their respective record(s).

19. The HIC sends the incident resolution detail to the HINP.
20. The HINP creates or updates the Incident Record (Appendix B) with the resolutions in the Incident Registry (Appendix C).
21. The client receives notification from the HIC regarding the privacy breach of their respective record(s).

POLICY COMMUNICATION

Not Listed