Corporate Policy

Communication - Protection of Privacy and Confidentiality of Information

Approved by:	Council	on	July 8, 2002
Report No.:	CL-30-02	Effective:	July 8, 2002
Reviewed:	April 13, 2012	Amended:	
Next Review:	April 2014	Note:	

Purpose:

To protect the privacy and confidentiality of corporate and personal information as it relates to the City of Burlington, including employees' personal information.

Policy Statement:

1) The City of Burlington, its Council, staff and volunteers will comply with Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

2) The City of Burlington will not sell personal and/or confidential information.

3) When the City sells software, it will ensure that all data is removed prior to the release of the software.

4) Information that can be manipulated or linked to other information to identify an individual will not be released.

5) All information is governed by this policy whether or not the information is recorded. Factual test data and live data are both included within this policy.

6) The collection of information by the City of Burlington will be governed by City policies, including the Records Retention By-law.

7) Actions arising from this policy will be reported to Management Committee on an annual basis.

8) The City of Burlington's Web site contains links to other Web sites. The City of Burlington is not responsible for the privacy practices of such Web sites.

9) The following disclaimer will be placed on all faxes and automatically on all e-mails being sent externally:

> This message, including any attachments, is privileged and intended only for the addressee(s) named above. If you are not the intended recipient, you must not read, use or disseminate the information contained in this email/fax. If you have received this e-mail/fax transmission in error, please notify the sender immediately by telephone, fax or e-mail and permanently delete this e-mail from your computer/shred this fax, including any attachments, without making a copy. Access to this e-mail/fax by anyone else is unauthorized. Thank you.

10) Staff, Council and volunteers must place the disclaimer noted above at the top of all private and/or confidential e-mails being sent internally.

Password Protection

- Electronic records containing personal/private information should be stored in password-protected files, whether the data is stored on a computer hard-drive, diskette or CD.
- Access to home computers and laptops that contain personal/private information should be password-controlled. Power-on passwords are to be employed for all laptop computers and personal digital assistants.
- Passwords shall not be recorded by any means unless they are stored in a secure fashion. Recorded passwords must at least be stored within a locked cabinet that has limited access, or within an appropriately encrypted file that has limited access

Scope:

This policy applies to all staff and members of Council

Definitions:

For the purpose of this policy, unless otherwise stated, the following definitions shall apply

Term	Definition
Record	Paper or electronically formatted databases, memos, policies and procedures, correspondence, reports, e-mails, faxes, handwritten notes to file.
Confidential	This description is given to all records and information with limited access and intended solely for the addressee(s). It includes records subject to solicitor-client privilege, records containing advice to government and sensitive or personal information. By the Municipal Act, subject matter related to: • the security of the city's property, • personal matters about an identifiable individual, • proposed or pending acquisition of land, • labour relations or employee negotiations, • litigation or potential litigation, • advice that is subject to solicitor-client privilege and • subject matter related to consideration of a request under MFIPPA are all considered in closed meetings. This information is to be labeled CONFIDENTIAL. Within the City's e-mail system, identified delegates are able to read these items. Note that confidential information and records may be releasable under MFIPPA legislation
Personal Information	• Any information about an identifiable individual, including race, national or ethnic origin, color, religion, sexual orientation, gender, marital or family status, age, address, telephone number, medical, psychiatric

Term	Definition
	or psychological, criminal or employment history, fingerprints, blood type and other information. • Any identifying number or symbol assigned to an individual. • Private or confidential correspondence sent to the City by an individual and replies that reveal the contents of the original correspondence. • Their personal opinions or views. • The opinions or views of another individual about the individual.
Personal Health Information	• information that identifies the individual, can be manipulated to identify the individual or can be linked or matched so as to identify the individual • information that relates to the physical or mental health of the individual • information that relates to providing health care to the individual • a plan or service (Long Term Care Act) and/or payments or eligibility for health care • information related to donation of body parts, substances or is derived from testing or examining the same • the individual's health number • information that identifies a provider of health care to the individual or a substitute decision-maker of an individual
Private Information	Is labeled **PRIVATE AND CONFIDENTIAL.** Within the City's e-mail system, delegates do not have

Term	Definition
	access to read “private” items and can read “confidential” items. Personal information is one form of private information.
Municipal Freedom of Information and Protection of Privacy Act MFIPPA	Council, staff and volunteers must comply with the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990. The Act protects the privacy of personal information about individuals. It contains rules about the collection, retention, use, disclosure and disposal of personal information held by government.

Performance Standards:

- Do not store personal/private information on a commonly accessed network drive.
- Remove records containing personal information from the office only if it is absolutely necessary to carry out your duties.
- When possible, leave original documents in the office and remove only copies of information.
- Keep paper records securely covered in file folders and contained in a locked briefcase or sealed box, under your constant control.
- In the office, lock records in a restricted area, and in a filing cabinet or desk drawer when not being used. At home, keep work-related records separately in only one location.
- Keep diskettes and CDs containing personal/private information under constant control while in transit and when working away from the office.

- If it is necessary to fax or photocopy personal information, do so yourself or ask an administrative staff person who is responsible for handling confidential materials to do it for you.
- When sending email containing private/confidential information, classify the e-mail using “Option” features.
- Confidential information must be prominently labeled CONFIDENTIAL on each page.
- Yellow paper must only be used for confidential matters.
- Confidential information must be disposed of by shredding not recycling.
- Information that is “Eyes Only” must be sent through standard mail procedures for sending private information. Do not use e-mail for eyes only information, including personal and health information.
- Even during meals and other breaks, keep files under your control. If impossible to keep with you, store records temporarily in a secure location (locked room or locked drawer).

References:

- Information Technology Security policy
- Information and Privacy Commissioner, Ontario www.ipc.on.ca

Roles

Accountable:

The City Clerk is answerable for the timely review, updating and dissemination of the policy.

Responsible:

All staff and Council must adhere to this policy.