BRAMPTON
Flower City
brampton.ca

Corporate Policies

SECTION: Terms and Conditions of Employment SUBJECT: **Information Technology Use**			POLICY 2.11.0
EFFECTIVE: May 16, 2011	REPLACES: Version approved March 24, 2003		PAGE 1 of 9
APPROVED BY: SMT – March 17, 2011		PROCEDURAL UPDATES: None	

POLICY CONTENTS

BACKGROUND

The Corporation is committed to promoting appropriate and responsible use of technology in order to enable a productive working environment for all City of Brampton (City) information technology users and to improve customer service internally across departments and externally to the public.

PURPOSE

This policy has been established to provide guiding principles including but not limited to awareness, usage behaviour, compliance, consistency, keep current with technology trends and to govern the acceptable use of computers, systems, mobile communication devices, electronic communication, telephones, servers, applications, data, software tools, accounts, information assets and/or network resources, (collectively referred to as “Information and Communication Technology”) at the City in conjunction with its established culture of good ethical behaviour, trust, and integrity.

Users of the City’s Information and Communication Technology must comply with this policy and all other City policies and related Standard Operating Procedures (SOPs) to ensure appropriate and responsible use of Information and Communication Technology.

SCOPE

This policy applies to all and any persons or entities that have access to and/or make use of the City’s Information and Communication Technology in any form or plan (collectively referred to as “User or Users”); except anonymous persons (e.g. people surfing the City’s public website).

This policy applies to Information and Communication Technology owned or leased by the City, and to authorized third-party devices that connect to the City’s network or reside on City-owned facilities.

PROVISIONS

1. General Acceptable Technology Use

1.1 Every user needs to exercise good judgment on the appropriate use of the City’s Information and Communication Technology in accordance with legislation, the City’s by-laws, corporate policies and/or related SOPs.

1.2 The utilization of the City’s Information and Communication Technology shall be reserved for conducting City business and shall not be used for any unlawful or prohibited purposes, whether explicitly identified herein or reasonably deemed unlawful or prohibited.

1.3 For security, compliance, and maintenance purposes, authorized staff may monitor and audit equipment, systems, and electronic communication. Unauthorized software, hardware or devices that may interfere with the corporate Information and Communication Technology or deemed malicious, may be disabled, disconnected and/or confiscated without notice.

1.4 Information and Communication Technology are made available to City users for business purposes. Although occasional personal use might occur, usage should not impact work productivity or interfere with work performance. Users are encouraged to ask their direct supervisor or the IT-Service Desk if they have any questions on the appropriate use of the Information and Communication Technology.

1.5 Exceptions under this policy may apply for a valid business need, with proper approval, from your management and the Chief Information Officer (CIO).

2. Access to Technology

Users accessing the City’s Information and Communication Technology must adhere to the Information Technology Security Guidelines and the following provisions:

2.1 Be responsible for the security of accounts under their control and to keep their password secured at all times, and shall not:

2.1.1 Share account or password information with anyone, including other employees, third-party, family, or friends; and/or

2.1.2 Provide access to another individual, either deliberately or through a failure to secure such access.

2.2 Ensure that City-owned information assets remain within the control of the City at all times. The storage of City-owned information on unauthorized devices is prohibited.

2.3 Be responsible for the security and appropriate use of City Information and Communication Technology under their control and shall not be used for any of the following:

2.3.1 Circumventing security, user’s log-in credentials (e.g. User ID and Password) or causing a security breach;

2.3.2 Accessing Information and Communication Technology and/or accounts without proper authorization;

2.3.3 Downloading or introducing inappropriate content or software with intentions to probe, scan, cause harm or loss or damage to the City's Information and Communication Technology;

2.3.4 Causing a disruption of service to the City's Information and Communication Technology, by performing non-business activities including but not limited to, gaming, audio/video downloading or play back, storing non City data, moving or disconnecting shared devices under the control of the City; and

2.3.5 Violating copyright law, and /or contractual obligations including, but not limited to, illegally duplicating or transmitting copyrighted or restricted software and content such as data, pictures, music, video, etc.

In addition, users must not engage in any other activity not explicitly stated herein but reasonably deemed to be unlawful or prohibited.

3. Protection of Physical Technology Assets

Users are responsible:

3.1 For the physical technology assets under their control including, but not limited to, computer systems, telephones, mobile devices, technology peripherals and accessories (e.g. printers, scanners, keyboard/mouse, speakers, software, etc.) in accordance with the Care, Custody and Control of City Assets Policy.

3.2 To secure and ensure the protection of assigned City Physical Technology Assets; and

3.3 To promptly report to the IT-Service Desk any theft of, or damage to, the assigned Physical Technology Assets.

4. Electronic Communication

4.1 Users shall ensure the appropriate use of electronic *communication resources* under their control.

4.2 Users are encouraged to keep their "contacts" information current to avoid the wrong distribution of their messages to the un-intended audience. Marking messages confidential, private or important is recommended.

4.3 The following electronic communication use is strictly prohibited:

4.3.1 Inappropriate use of electronic communications, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates legislation (e.g. Municipal Freedom of Information and Protection of Privacy Act-MFIPPA) and/or City's by-laws, policies or SOPs (e.g. Workplace Harassment Prevention) or the safeguarding of confidential or proprietary information;

4.3.2 Sending Spam via e-mail, text messages, instant messages, voicemail, or other forms of electronic communication; and/or

4.3.3 Forging, misrepresenting, or obscuring user identity on any electronic communication to mislead the recipient.

5. Social Media

5.1 Use of Social Media shall be primarily for City-related business and in accordance with the City's Standard Operating Procedure (SOP) for Use of Social Media for Business Purposes. Although occasional personal use might occur, usage should not impact work productivity or interfere with work performance. Use of Personal Social Media across the corporation can be monitored and usage reports on an aggregate and individual user basis will be available to management. Users are reminded to ask their direct supervisor if they have any questions about appropriate uses of Social Media.

5.2 In general, users must use good judgment and exercise common sense when using Social Media Networks or Outlets and adhere to the City's Employee Code of Conduct or the Code of Conduct for Members of Council, or per provisions outlined in relevant contractual or service agreements.

5.3 Personal Use of Social Media:

Users as citizens have the right to voice their opinion, on their own time and risk; however, users shall not:

5.3.1 Use their City's e-mail account or City's contact information on their Personal Social Media Outlets;

5.3.2 Identify themselves as City employees or affiliated with the City in any manner to represent the City or use confidential City information;

5.3.3 Communicate or engage in any conversations that relate to their work at the City in a negative or destructive manner;

5.3.4 Represent personal opinions as those of the City (or department, division…etc.) or criticize internal corporate policies, SOPs of the City; and/or

5.3.5 Launch personal attacks or make defamatory or offensive (racist, sexist, lewd…etc.) statements or making partisan or political comments related to the City.

6. Electronic Data and Intellectual Property

6.1 All *Information Assets* shall remain the intellectual property of the City and should be used in accordance with corporate policies, SOPs, relevant licenses, contractual terms and conditions.

6.2 Users shall take all reasonable precautions to protect the information assets of the City. Information Assets that are generally made available to the public, service providers or third-party working with, or on behalf of, the City must be appropriately protected either through non-disclosure, contractual agreement, or appropriate disclaimer indemnifying the City.

6.3 Distribution of these information assets are subject to legislation, City's by-laws, policies, SOPs and/or provisions outlined in contractual agreements.

6.4 Information Assets authorized for release to the public are subject to its prospective terms and conditions of use and must meet the City's Open Data Guidelines (Coming Soon).

7. Applications and Systems

Users who have advanced system and application privileges to administer, configure, support or have the ability to cause any changes to City Applications, Data or Systems must adhere to the Information Technology Applications and Systems Guidelines (Coming Soon).

8. Electronic Records Management

All electronic records are to be managed and maintained in accordance with the City's Records Management Policy and Records Retention By-law, as amended.

9. Acquisition of Information and Communication Technology

9.1 All acquisition of Information and Communication Technology shall be in accordance with the City's Purchasing By-law, Purchasing Card Policy, and the provisions outlined in relevant master/contractual agreements, purchase orders and/or statements of work.

9.2 Users are encouraged to review the IT Service and Standards Catalogue (Coming Soon) or contact the IT-Service Desk for information on Information and Communication Technology acquisitions.

10. Enforcement and Monitoring Controls

10.1 The City monitors and/or logs access and usage activity of the City's Information and Communication Technology to ensure use in accordance with this policy, the MFIPPA and the City's Privacy Statement.

10.2 The City reserves the right to revoke or block access and/or usage of any Information and Communication Technology if deemed necessary, with or without notice.

11. Actions for Non Compliance

11.1 Users in violation of this Policy will be reported to the appropriate level of management and/or the CIO.

11.2 Violators of this policy may be subject to disciplinary actions up to, and including, termination of employment or contract in accordance with the City's Employee Code of Conduct or per provisions outlined in relevant contractual or service agreements.

11.3 Violators for unlawful purposes may be subject to criminal prosecution, civil liability or both.

ADMINISTRATION

Users' Acknowledgement:

1. Users are required to acknowledge this policy on an annual basis.
2. Contractors and affiliated entities will be required to acknowledge this policy as part of their contract, service or affiliation agreement.

CONTACT

IT-Service Desk
Information Technology Division,
Financial and Information Services Department,
City of Brampton
2 Wellington St. West 2nd floor
Brampton, Ontario L6Y 4R2
Telephone: 1 (905) 874-2029
e-Mail: helpdesk@brampton.ca
Policy URL:

http://ourbrampton.brampton.ca/KnowledgeCentre/PoliciesSOPsAndMasterPlans/Administrative%20Policies/2.11.0%20Information%20Technology%20Use%20Policy.pdf

Links to Supporting Documents:

1. Information Technology Security Guidelines
2. Care, Custody and Control of City Assets Policy
3. Municipal Freedom of Information and Protection of Privacy Act-MFIPPA
4. Workplace Harassment Prevention
5. Use of Social Media for Business Purposes
6. Open Data Guidelines
7. Employee Code of Conduct
8. Code of Conduct for Members of Council
9. Information Technology Applications and Systems Guidelines
10. Records Management Policy
11. Records Retention By-law 163-2008
12. Purchasing By-law
13. Purchasing Card Policy
14. IT Service and Standards Catalogue
15. Privacy Statement

GLOSSARY OF TERMS

Term	Meaning
Account or Accounts	That combination of user ID and password that provides an individual with access to a computer system or computer network.
Anonymous	Without name or way to distinguish one person or action from one another.
Block monitoring	A software or tool that interferes or ceases the functionality of the City's Information Technology monitoring tools
Electronic Communications	Any electronic method used to communicate, including but not limited to electronic mail, the Internet/World Wide Web, video recordings, facsimiles, pagers, telephones, cellular text messages, Blackberry Messenger, Blackberry PIN, etc.
Information Assets	Including but not limited to data/software and/or electronic documents, electronic communication written and/or developed by users related to their work at the City.
Information and Communication Technology	Computers, systems, mobile communication devices, telephones, servers, applications, data, software, technology tools, accounts and/or network resources
Instant Messages (IM)	Sending real time messages to another Internet user. Also referred to as IM.
Intellectual Property	Something produced by the mind, of which the ownership or right to use may be owned by the organization in which a person is employed or engaged to work for and may be legally protected by a copyright, patent, trademark, etc.
Monitoring	A standard practice by information technology resource administrators of reviewing transaction activity and other similar logs generated by the system/network, analyzing performance anomalies and traffic patterns, and/or running programs designed to identify the source of a specific problem, alarm or pattern potentially indicative of illegal or inappropriate use.

Term	Meaning
Open Data	Certain data sets that are freely available to everyone, without restrictions from copyright, patents or other mechanisms of control
Physical Technology Assets	**Including, but not limited to, computer systems, telephones, mobile devices, technology peripherals and accessories (e.g. printers, scanners, keyboard, speakers, etc.)**
Security Breach	External act that bypasses or contravenes the City's IT Technology Use Policy or Security Guidelines.
Social Media	Social media are works of user-created video, audio, text or multimedia that are published and shared in a social environment, such as a blog, podcast, forum, wiki or video hosting site. More broadly, social media refers to any online technology that lets people publish, converse and share content online`.
Social Media Networks or Outlets	Social networking is the act of socializing in an online community. A typical social network such as Facebook, LinkedIn, MySpace or Twitter allows you to create a profile, add friends, communicate with other members and add your own media.
Spam	Indiscriminate mailing or forwarding of unsolicited e-mail to a larger group of users.
User or Users	All and any persons or entities that have access to and/or make use of the City's Information and Communication Technology in any form or plan except anonymous persons (e.g. people surfing the City's public website)