City of Mississauga

Corporate Policy & Procedure

MISSISSAUGA

Policy Title: Access To and Acceptable Use of Information Technology Resources

Policy Number: 03-05-01

Section:	**Corporate Administration**	Subsection:	**Technology**
Effective Date:	**June 9, 2010**	Last Review Date:	**[Last Review]**
Approved by: **Council**		Owner Division/Contact: **Information Technology Division, Communications Division** **Corporate Services Department**	

Policy Statement

The City of Mississauga provides access to various types of Information Technology Resources for business purposes and expects that all Information Technology Resources will be used appropriately and in accordance with this policy.

Purpose

The purpose of this policy is to outline the City's expectations with respect to the access and acceptable use of Information Technology (IT) Resources provided by the City of Mississauga and to ensure IT Users are aware of their responsibilities and the limitations regarding privacy and confidentiality when accessing and using IT Resources. The accompanying "Guidelines for Acceptable Use of IT Resources" (the Guidelines) reinforce and expand on the information provided in the policy.

Scope

This policy and accompanying Guidelines apply to all City employees, elected officials, citizen members of committee, and volunteers acting on behalf of the City, as well as affiliates, contractors, consultants and any other individuals given authorized access to, and use of, City IT Resources. All authorized IT Users are expected to respect the intent of this policy.

IT Resources must be used in compliance with this policy, applicable laws and regulations, professional standards, software licensing agreements and Corporate Policies and Procedures, including but not limited to the following Human Resources, Employee Conduct policies:

- Standard of Behaviour
- Respectful Workplace
- Fraud and Theft
- Conflict of Interest

Definitions

For the purposes of this policy:

"E-mail" includes all business and personal communications created using or accessing the City's E-mail system, regardless of physical location, and includes E-mail communications sent or received on any City-issued or City-authorized Wireless Communication Device or smart phone, including, but not limited to, a BlackBerry®, iPhone™, or cell phone. E-mail includes communications sent or received on any personally owned Wireless Communication Device, as well as to externally hosted e-mail sites, when the communication is conducted on behalf of/pertains to City business.

"Internet use" includes all activities undertaken on any electronic device through the City's Internet resources, including electronic mail and browsing and/or posting information to internal or external websites, whether accessed from a City facility or any offsite location.

"Information Technology User" (IT User) includes all employees, elected officials, citizen members of committees and volunteers acting on behalf of the City of Mississauga, as well as all affiliates, contractors, consultants and any other individuals given access to, and use of, City IT Resources.

"Information Technology (IT) Resources" means City owned or issued IT resources including, but not limited to:

- Hardware, such as computer desktops, laptops, portable and computing devices and related peripherals (e.g. Printers, scanners, etc.) And wireless communication devices (e.g. Blackberry®, pagers, iPhone™, smart phones, cell phones, etc.)
- All internet and e-mail systems
- Electronic data transmission equipment, devices and networks
- Business systems and servers and all city managed data and software
- All types of telephone, radio and other audio/voice or audio/visual communication equipment, devices and networks, including voicemail
- Local and network storage media used in the operation of these resources including, but not limited to, diskettes, CDs, tape media, paper, USB, flash memory, flash drives, external hard drive, etc., and
- Data, information and other work products, such as computer programs, databases, spreadsheets, etc., created and/or maintained in using these resources

In addition, any city related data and information that is accessed, stored, created, processed, transmitted or filed in a personal electronic device is included in this definition

"Wireless Communication Device" means any cordless device that is capable of receiving or transmitting telephone communications, electronic data, mail, instant messaging (e.g. PIN

messaging) or texting and includes, but is not limited to, cell phones, iPhones™, smart phones, pagers, and a BlackBerry®.

Administration

Access to IT Resources is provided on a corporate basis through the Information Technology Division of the Corporate Services Department.

The Director of Information Technology shall designate security administrators for each corporate system. The security administrators will be responsible for implementation of appropriate security controls.

The parameters for corporate-wide, routine monitoring are set by the Director of Information Technology in consultation with all City departments and approved by the Commissioner of Corporate Services & Chief Financial Officer (CFO) and the City Manager. Modification to these parameters must be conducted according to established protocol, documented, and approved by the Commissioner of Corporate Services & CFO and authorized, in writing, by the City Manager.

Segregation of Duties

There must be a segregation of duties between individuals responsible for configuring the system parameters and those who are responsible for the routine administering of the internet monitoring software. Appropriate authorization must be obtained before system parameters are reconfigured.

Legislative Requirements

Municipal Freedom of Information and Protection of Privacy Act

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) governs the collection, use and disclosure of information by the City. MFIPPA applies to information both in hard copy and electronic form. Therefore, communications created, received or transmitted using the City's IT Resources, including personal records, may be subject to the provisions of MFIPPA. Elected officials' records are dealt with in accordance with the Corporate Policy and Procedure - Records Management - Elected Officials' Records.

Communications, including E-mail, text or PIN messages sent or received from any IT Resources, including a BlackBerry®, may be subject to MFIPPA and to the same retention requirements as hard-copy messages and must be dealt with in accordance with the City's Records Retention By-Law 537-96, as amended from time to time or, in the case of elected officials' records, in accordance with Corporate Policy and Procedure - Records Management - Elected Officials' Records.

Guidelines for Acceptable Use of It Resources

The City's "Guidelines for Acceptable Use of IT Resources", available through departmental IT Managers and on the City's Intranet, and provides assistance to IT Users in understanding their respective responsibilities and the City's standards and expectations. The purpose of the Guidelines is to protect the integrity of City IT Resources and the safety and security of IT Users by offering additional information and examples of both acceptable and unacceptable use of IT Resources.

Ownership and Privacy Expectations

Ownership

All IT Resources acquired and managed by the City and the data, documents, information and work product created, received, transmitted or downloaded from external sources using the City's IT Resources are the sole property of the City of Mississauga.

Privacy and Monitoring

The City reserves the right to implement reasonable technological and procedural measures in order to ensure compliance with corporate policies and standards, assess system or network performance and resource usage, and protect and maintain the security of IT Resources, as well as safeguard the integrity of IT Users.

IT Users should have no expectation of privacy in relation to the use of IT Resources and should be aware that their use of IT Resources, both business and personal, may not be confidential and may be subject to MFIPPA. The City reserves the right to monitor and/or access any electronic voice or data file and may do so for any of the following reasons:

- Routine monitoring of the City's computer systems to track and analyse trends of operational metrics, which includes tracking of web site visits
- Appropriate City staff, who are governed by confidentiality agreements, may be authorized and/or required to access the information to meet legal obligations or if there are reasonable grounds to suspect that an IT User has abused or contravened this policy, and
- To protect the City's interests in the event of a reasonable suspicion of crime or inappropriate use of City IT Resources, and
- If there are any other legitimate authorized reasons to do so, such as retrieving voice mail directly from an Employee's telephone in the event of an unscheduled absence or unexpected departure from the City; approval from the Director of IT is required

Any resulting investigation into an IT User's use of IT Resources must be authorized according to the Investigation section of this policy.

Confidential Information

Employees are advised that the privacy of information sent electronically that is sensitive or confidential in nature, such as personal information about individuals; employee performance or other human resource issues; information regarding issues to be discussed in camera, cannot be guaranteed. IT Users should consider another medium, such as sending the information via interoffice mail in an envelope marked “Confidential”. When sensitive or confidential messages are sent electronically, both the sender and the receiver are responsible for safeguarding the information.

Personal communications which IT Users do not want accessed or monitored in accordance with this policy should not be retrieved, created, or transmitted using the City’s IT resources.

IT Users may forward communications in electronic format to other IT Users or external clients/customers as required, subject to protecting any confidential information or information which is otherwise protected by MFIPPA. IT Users who send communications in electronic format and do not want those communications forwarded by the receiver(s) should expressly indicate this in the subject line or at the top of the e-mail by marking the electronic communication with “Do Not Forward”. If an IT User receives communication in electronic format which is marked “Do Not Forward”, it must not be forwarded unless express authorization has been received from the sender.

Responsibilities

IT User Responsibilities

IT Users are expected to exercise good judgement when using IT Resources and to ensure they are used appropriately. Any abuses of IT Resources must be reported to the individual’s immediate supervisor or the Director of IT and the departmental HR Manager.

IT Users are responsible for the security of mobile equipment assigned to them. Employees using a City laptop, external hard drive, USB memory stick, digital memory card, portable device or Wireless Communication Device are responsible to protect both the equipment and data, inside and outside of the office. Information which is sensitive or confidential in nature should not be stored on mobile equipment, whether City provided or personally owned. Where it is necessary, the information should be password protected or, when possible, encrypted. Loss or theft of any City issued equipment must be reported immediately to the employee’s immediate supervisor, the departmental IT Manager, the Access and Privacy Officer and Corporate Security.

Supervisor/Manager Responsibilities

Supervisors/managers are responsible for ensuring that IT Users under their supervision are aware of and comply with this policy; are properly authorized and trained to use IT Resources; that the access rights of IT Users who transfer, take a leave of absence exceeding three weeks,

or leave the City are processed or rescinded in a timely manner; and that all IT Resources are returned to the City, if applicable.

City departments, and therefore supervisors/managers, are responsible for equipment security. Where practical, small, portable equipment should be locked up at night and, depending on the level of risk, other methods such as restraining devices should be used, particularly in remote locations. Any theft, tampering or unacceptable use of IT Resources must be immediately reported to the appropriate departmental HR Manager and/or the Director of IT.

Supervisors/managers are accountable to review IT usage reports generated by the IT Division and to address atypical results with IT Users, if applicable.

IT Division Responsibilities
The IT Division of the Corporate Services Department is responsible to administer, distribute and track the location of required IT Resources; provide ongoing training, guidance, technical support and assistance to IT Users on efficient IT practices; and to ensure the Guidelines remain current.

IT Division staff are also responsible for verifying that the City's IT Resources are efficient and appropriate for the needs of the Corporation and will administer the programs used to conduct the on-going authorized collection and monitoring of IT User activity, including generating IT usage reports. The IT Division’s monitoring and routine reporting of IT Users’ activities are the responsibility of the Director of IT.

Communications Division Responsibilities
The Communications Division of the Corporate Services Department is responsible for the overall look of the City’s Internet site and for monitoring the content of the site to ensure that standards are met. Standards for the design of corporate web pages (page layout, colours, fonts, etc.) have been developed in consideration of accessibility for all IT Users. Individual departments must comply with these standards.

Communications will also be consulted by the Director of IT if consideration is being given to a departmental request to host a corporate web page through another service provider.

Access

Access
IT Users may not authorize their own IT Resources access. Access to City IT Resources is determined by the requirements of the IT User’s position. It is the responsibility of individual departments to assess IT Users needs when granting access. Form 990 - Security Access must be completed, authorized and signed by the employee’s immediate manager or designate and forwarded to the applicable departmental IT Manager for approval and processing. Alternately,

the Director of IT may provide authorization. In the case of elected officials, the form must be approved by the Commissioner of Corporate Services & CFO.

Access for any authorized IT User who is not an employee or elected official requires the approval of the Director of IT or their designate. Authorized IT Users will be required to sign an acknowledgement of these requirements and may also be requested to sign a confidentiality agreement, if applicable.

Where access to an information system that is not managed by the department requesting access, supplementary authorization by the Director of Information Technology or the applicable Departmental Commissioner or designate will also be required.

Exceptions
The Director of IT may authorize access to IT systems to allow Information Technology staff to support maintenance, operations and investigations on specific systems. However, prior to any investigation, the Director must seek the necessary authorizations in accordance with the Investigation section of this policy.

In accordance with the City's Emergency Plan, the Director of IT may authorize Information Systems staff to access and update systems to deal with extraordinary circumstances. On cessation of the emergency, the Director shall withdraw and/or update privileges immediately. Detailed records of all updates shall be retained for audit purposes.

Use of It Resources

Business vs. Personal Use
The primary purpose of IT Resources is for City business communication and related activities. Occasional or incidental personal use of IT Resources is permitted within reasonable limits, provided it does not conflict with business use or time, impact negatively on other IT Users or on IT Resources, or adversely affect an individual's performance of work duties and responsibilities. IT Users are responsible for exercising good judgement regarding the reasonableness of personal use. IT Users are reminded that personal use may be monitored and accessed in accordance with this policy.

Use of the City's IT Resources to run a personal business is strictly prohibited. This includes photocopying or printing flyers, advertisements, etc. for a personal business or for personal gain, or sending "for profit" messages via the Internet. Further, it is a contravention of Corporate Policy and Procedure, Human Resources, Employee Conduct, Conflict of Interest.

No information should be distributed which would not be distributed under the City's letterhead or logo and no information should be viewed, copied or saved which is not related to City business.

Information which would not be released in hard copy form should not be released in electronic form.

It is the employee's responsibility to reconcile any outstanding overage charges such as personal long distance. For additional information, refer to Corporate Policy and Procedure, Corporate Administration, Technology, Personal Telephone Charges.

The City cannot guarantee the security of online financial transactions such as, but not limited to, personal online banking. IT Users must therefore be aware that they perform these transactions at their own risk. Refer to the Guidelines for additional information.

Passwords

Passwords prevent access to equipment or confidential data by unauthorized persons, without impeding sharing of information or exchange of corporate data among departments by authorized staff. IT Users must use and safeguard their individual passwords at all times.

General Restrictions

IT Resources may not be used for transmitting, accessing, retrieving, viewing, uploading, downloading or storing inappropriate communications. This includes, but is not limited to, discriminatory, harassing, threatening, profane, malicious, pornographic or illegal communications. Inadvertently accessing an inappropriate site, or receiving an e-mail with an unacceptable attachment, will not be considered a violation of this policy. However, printing, saving or forwarding inappropriate material is a violation.

IT Users must respect copyright restrictions on any downloaded information.

The files or data of other IT Users may not be accessed, deleted or modified without the IT User's consent, or in accordance with this policy.

IT Users may not install or download software on any City issued IT Resource without the prior knowledge, approval and authorization of their departmental IT Manager. Copying licensed software is strictly prohibited; only software that is licensed with the City of Mississauga and paid for through the designated channels is permitted.

Internet service is provided on a corporate basis through the IT Division of the Corporate Services Department. Individual departments may not host corporate web pages through another service provider without the authorization of the Director of IT.

City staff posting information on external websites that relates to the City must not knowingly defame the City or post confidential information. This includes, but is not limited to, chat groups, blogs, message boards, Facebook, etc.

All IT Users are prohibited from sending credit card Primary Account Numbers (PAN) via E-mail or any other unencrypted electronic medium. Online purchasing with a City issued credit card (PCard) for City business purposes is permitted.

Web Board/Potpourri
The City's Web Board/Potpourri allows staff to post and exchange messages and have discussions with other City staff. Employees must exercise good judgement and post only items that are appropriate. Staff can post referrals, non-City related events, and personal items for sale/buy; however, Web Board/Potpourri cannot be used to promote an ongoing personal business. For additional information regarding Web Board/Potpourri, refer to the City's Intranet or the Guidelines.

Wireless Communication Devices – Safe Driving Guidelines
All IT Users who use Wireless Communication Devices in the performance of their duties are expected to use Wireless Communication Devices in a safe and responsible manner and in accordance with Corporate Policy and Procedure - Human Resources - Acceptable Use of Mobile Technology.

Acquisition of Goods and Services Through the Internet
Any acquisition of goods and services for business use must comply with the City's by-law governing purchasing, and established Corporate Policies and Procedures on Purchasing.

Removal of IT User Access and Return of IT Resources

Upon cessation of employment for any reason; at the end of an IT User's relationship with the City; or at any time upon request, the IT User will immediately return all IT Resources to the City. All information pertaining to the City stored solely on personal IT devices, such as but not limited to, laptops, USB, flash memory and external hard drives, remains the property of the City. All such information not already in the City's possession must be returned to the City and be immediately and permanently deleted from any home computer or personal IT device.

Compliance

Any IT User who violates this policy will be subject to appropriate disciplinary action, up to and including termination of employment. The City is authorized to immediately withdraw IT access and initiate an investigation should abuse of any aspect of this policy be suspected.
In addition, any expenses incurred as a result of non-compliance will be the personal responsibility of the IT User.

Investigation
Prior to commencing an investigation into the inappropriate use of IT Resources by an IT User,

authorization must be obtained from the Directors of IT and Human Resources and from the following individuals or their designates:

- Investigations concerning a citizen member of committee, from the City Manager
- Investigations concerning City staff, including managers and supervisors, from the applicable Director
- Investigations concerning a director, from the applicable commissioner
- Investigations concerning a commissioner, from the City Manager
- Investigations concerning the City Manager from the City Solicitor, and
- Investigations concerning an elected official, from the City Manager as authorized by Council

In addition, the appropriate commissioner must be notified of any investigation concerning their departmental staff.

All IT Users are required to fully cooperate in any investigation.

Revision History

Reference	Description
GC-0397-2010 2010 06 09	
September 25, 2013	Housekeeping – title change for Commissioner of Corporate Services