SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **1 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

TABLE OF CONTENTS

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **2 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

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 governance and awareness for the acceptable use of computers, systems, mobile communication devices, electronic communication, telephones, servers, applications, data, software tools, electronic access accounts, information assets, technology acquisition, technology standards and processes, network resources and the overall Business-Technologies and Infrastructure, (collectively referred to as Information and Communication Technology ("ICT")) at the City in conjunction with its established culture of good ethical behaviour, trust, and integrity.

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

SCOPE

This policy applies to all and any persons or entities that have access to and/or make use of the City's ICT in any form or plan (collectively referred to as "User or Users"); except anonymous persons (e.g. unidentified people who are visiting and accessing the City's public website).

This policy applies to ICT owned or leased by the City or those that are not owned by the City but are certified, contracted or permitted to connect and access the ICT through approved processes, remote access tools, or programs such as Bring Your Own Device ("BYOD") Program.

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **3 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

PROVISIONS

1. General Acceptable Technology Use

1.1. Every User needs to exercise good judgment on the appropriate use of the City's ICT in accordance with legislation, the City's by-laws, corporate policies and/or related SOPs.

1.2. The utilization of the City's ICT 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. ICT are made available to City Users for business purposes. Although occasional personal use might occur, usage should not be excessive, impact work productivity or interfere with work performance. Users are encouraged to ask their direct supervisor, their Departmental Business Services Office or the IT Service Desk if they have any question regarding the appropriate use of ICT.

1.4. 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 this corporate policy or deemed malicious, may be disabled, disconnected and/or confiscated without notice.

1.5. Exceptions to this policy must be approved by the Chief Information Officer (CIO), or authorized delegates. An "Exception to Policy Request" must include valid business justification and documented approvals from the requestor's Divisional Head.

2. Access to Technology

Users accessing the City's ICT (within the office or remotely) must adhere to the IT Security Governing Principles and the following provisions:

2.1. Be responsible for the security of account(s) under their control and to keep their password secured at all times;

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **4 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

2.2. Shall not share such account(s) or password information with anyone, including other employees, third-party, family, or friends;

2.3. Shall not provide unauthorized access to another individual, either deliberately or through failure to secure such access.

2.4. 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.

2.5. Reasonable use of and access to personal devices, accessories and digital information are not restricted to City owned or leased end-user computing devices such as (Laptop, Desktop, Tablet or Smart Phone). The storage and use of personal multimedia, files and/or tools on City's file shares or shared data repositories are prohibited.

2.6. Be responsible for the security and appropriate use of City ICT under their control; and shall not be used for any of the following:

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

2.6.2. Accessing ICT and/or accounts without proper authorization;

2.6.3. Downloading or introducing inappropriate content or software with intentions to probe, scan, cause harm or loss or damage to the City's ICT;

2.6.4. Causing a disruption of service to the City's ICT, 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

2.6.5. Violating copyright laws, 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.

2.7. Users who manage and use generic system account(s) to administer business processes and controls are accountable at all times to safe guard the use of such account(s); refrain

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **5 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

from impersonating or misuse of these account(s) to hide their identity; and/or share these account(s) with others for same.

2.8. All 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, computing devices and 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 need to be aware of and comply with the City's Personal Information Protection Policy when using personally owner technology resources to access the City's ICT for City related business.

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

4.3. Users are encouraged to keep their contact information current to avoid the wrong distribution of their messages to the un-intended audience. Marking messages as "confidential", "private" or "important" is recommended and shall not be confused with the use of federal classification of information as "confidential", "secret" or "top secret".

4.4. The following electronic communication use is strictly prohibited:

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **6 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

4.4.1. Inappropriate use of electronic communications,

4.4.2. Supporting illegal activities,

4.4.3. Procuring or transmitting material that violates legislation (e.g. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), Canada Anti-Spam Legislation (CASL) City's by-laws, policies or SOPs (e.g. Workplace Harassment Prevention), or safeguarding of confidential or proprietary information;

4.4.4. Sending Spam via Email and/or unsolicited commercial electronic messaging (CEM), text messages, instant messages, voicemail, or other forms of electronic communication; and/or

4.4.5. Forging, misrepresenting, or obscuring User identity on any electronic communication to mislead the recipient;

5. General Use of Mobile Communication and Computing Devices:

5.1. This section applies to Users who: (i) have been issued a Mobile Communication and Computing Device(s) (Mobile Devices) by the City; or (ii) participate in the City's Bring Your Own Device (BYOD) Program. However it does not apply to the use of personal stationary computing devices connected via remote access to the City's ICT such as home desktop personal computer(s).

5.2. Each User is expected to use good judgement and act in accordance with the City's Employee Code of Conduct or the Code of Conduct for Members of Council (as applicable to each User) when using Mobile Devices to conduct City related business.

5.3. Users are reminded to ask their direct supervisor, Departmental Business Service Office or the IT Service Desk if they have any questions about appropriate uses of any mobile communications device that is being used (in whole or in part) for City related business.

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **7 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

5.4. Usage of any mobile communications device to perform work outside of the User's regular working hours must be approved by the User's supervisor in accordance with the City's policies and procedures regarding overtime work. Neither being issued a mobile communications device by the City nor being approved to participate in the City's BYOD Program is in itself an approval to work overtime hours.

5.5. In the event that a mobile device is lost or stolen, the employee is to notify their manager/supervisor and the IT Service Desk as soon as possible to suspend the device immediately. A data wipe will then be activated on the lost or stolen City Issued mobile device which will completely remove all information contained on the device, City is not liable of loss of any personal or business data and/or tools on such devices.

6. Use of City Issued Mobile Devices:

6.1. Users who have a City Issued Mobile Devices must be aware of and comply with the City's Standard Operating Procedure for Mobile Communications,

6.2. During a User's working hours, usage of City Issued Mobile Devices for personal purposes should be limited and not used excessively; interfere with productivity or work performance.

6.3. Users may be held responsible for costs related to repairs to or replacement of damaged City Issued Mobile Devices as a result of their reckless or negligent actions.

7. Use of Personal Mobile Devices under the BYOD Program:

7.1. The City's BYOD Program is an optional convenience program and participation is voluntary;

7.2. Users' Divisional Head's and the CIO, or their delegates must approve the participation of such Users into the BYOD Program;

7.3. Users participating in the BYOD Program shall:

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **8 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

7.3.1. Agree to permit the City to install tools and apply reasonable controls to their Personal Mobile Devices in order to use the City's mobile services (as they become available), resources and information such as (WiFi and Email);

7.3.2. Adhere to the City's Standard Operating Procedure (SOP) for the BYOD Program.

7.4. Reimbursement for any related expenses or receiving of any monetary compensation for participating in the City's BYOD Program shall be determined in accordance with the City's Standard Operating Procedure for BYOD Program and related eligibility criteria.

7.5. During a User's working hours, User's use of Personal Mobile Devices for personal purposes should be reasonable and not interfere with the User's productivity or work performance.

7.6. The City may cancel or remove User(s) from the BYOD Program at any time, by giving such User(s) at least 30-days written notice.

7.7. The City reserves its rights to:

7.7.1. Modify and/or suspend services provided to participants of the BYOD Program at any time and without notice.

7.7.2. Monitor usage related to the use of Personal Mobile Devices for City's work purposes under the BYOD Program at any time and without notice.

7.7.3. To investigate improper use of Personal Mobile Devices under the BYOD Program at any time and without notice; violations will be reported to management and to authorities. Compliance to and order to surrender Personal Mobile Devices to City investigators or authorities will be expected and removal of City data, tools and controls may be performed, which may also wipe personal media and tools; In any event, the City shall not be held liable in whole or in part.

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **9 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

8. Social Media

8.1. 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.

8.2. Although occasional personal use might occur, usage should not impact work productivity or interfere with work performance.

8.3. 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.

8.4. Users are reminded to ask their direct supervisor if they have any questions about appropriate uses of Social Media.

8.5. Comments and messages posted to the City's official social networking sites are considered transitory records and will not be retained for any specified length of time.

8.6. The use of social media accounts and websites must adhere to the principles outlined in the MFIPPA.

8.7. 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.

8.8. 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:

8.8.1. Use their City's Email account or City's contact information to voice such opinions on their Personal Social Media Outlets;

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

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **10 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

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

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

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

9. Electronic Data and Intellectual Property

9.1. 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.

9.2. 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.

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

9.4. Information Assets authorized for release to the public are subject to its respective terms and conditions of use and must meet the City's Information Management Policy and Personal Information Protection Policy

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **11 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

10. Use and Administration of Applications and Systems

10.1. Users who have advanced system and application privileges to administer, configure, support or have the ability to cause any changes to City's Applications, Data or Systems must adhere to the IT Managed Services and the IT Security Governing Principles.

10.2. Support of Business-Technology Applications and Systems are subject to their respective Service & Operational Level Agreement(s) (SOLAs) per the IT Managed Services.

11. Electronic Records and Digital Data Management

11.1. All electronic records are to be managed and maintained in accordance with the City's Information Management Policy and Personal Information Protection Policy.

11.2. Governance and management of Digital Data throughout its lifecycle is essential to ensure protection, usability, and access in accordance with the City's Information Management Policy and Personal Information Protection Policy.

12. Acquisition of Technology

12.1. Acquisitions of Technology and ICT must adhere to:

12.1.1. The City's Purchasing By-law, and Purchasing Card Policy;

12.1.2. The provisions outlined in relevant master/contractual agreements, purchase orders and/or statements of work;

12.1.3. The City's IT Architectural Controls and Standards; also a copy of the CoB Technology Environment Architectural Standards must be attached as an appendix to all technology procurement documents for full disclosure purposes.

12.1.4. The City's IT Project Management and Program Delivery Governing Principles;

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **12 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

12.2. Acquisition of Technology and ICT must be pre-approved by the CIO, or authorized delegate(s) and retained on file for audit purposes;

12.3. Acquisition of printing devices must be pre-approved by the Manager of Facilities Support Services, Departmental Business Services Office or authorized delegate(s);

12.4. Upon approval of technology acquisition, the designated capital or expenditure account must be validated and authorized by the respective Divisional Head or delegate(s);

12.5. Users are encouraged to review the IT Service and Standards Catalogue or contact the IT Service Desk;

13. Use and Allocation of Printing Services:

13.1. Printer Allocation for each floor will be limited to the designated print areas, additional printers will only be issued under compelling circumstances and must be approved by the Manager of Facilities Support Services and the respective Divisional Head and respective Departmental Business Services Office, or authorized delegate(s).

13.2. Printer colour usage should only be applied to final documents, all draft and proofing documents should be printed in black & white and in draft mode.

13.3. Usage of shared printing and multifunctional devices are intended for day-to-day reasonable printing needs. All large print jobs that exceed one hundred (100) pages must be sent to the City's Digital Print Centre.

13.4. Users should use good judgement when printing emails and website content.

13.5. Users should take reasonable actions to reduce paper printing and print wastage, by applying electronic records management and sharing practices.

13.6. Users must adhere to the Corporate Printing Governing Principles, which also outlines best practices for print configurations, usage guidelines, and standard operating procedures related to the use of the City's Digital Print Centre.

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **13 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

14. Secure Electronic & Digital Signature (e-Signature)

14.1. The City of Brampton may permit and accept the use of Secure Electronic & Digital Signature referred to as "e-Signature" similar to live signature if it complies with the Secure Electronic Signature Regulation of Canada, this Policy and the IT Security Governing Principles.

14.2. Secure Electronic & Digital Signature must use:

(1) A digital signature certificate that is valid at the time when the data contained in an electronic document and is digitally signed,

(2) the certificate is readable or perceivable by any person or entity who is entitled to have access to the digital signature certificate; and

(3) has not expired or been revoked.

14.3. The City reserves the rights to reject the electronic signature without a reason or if the certificate authority does not meet the City's IT risk and standards or opinion.

14.4. An electronic signature using digital signature pads typically connected to point of sale terminals will be accepted on such transactions as long as is witnessed by the terminal operator and comply with MFIPPA and the City's Privacy Statement.

15. Enforcement and Monitoring Controls

15.1. The City typically monitors and/or logs access and usage activity of the City's ICT to ensure compliance with this Policy, the MFIPPA and the City's Privacy Statement.

15.2. The City reserves its rights to revoke or block access and/or usage of any ICT services or resources if deemed necessary, with or without notice.

16. Actions for Non Compliance

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

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **14 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

16.2. 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 or reporting processes in case of elected officials.

16.3. Violators for unlawful purposes may be subject to criminal prosecution, civil actions or both.

ADMINISTRATION

Users Acknowledgement:

Annual acknowledgement of this policy is mandatory.
Acknowledgement can be performed electronically or by signing the 2.11.0 Information Technology Use Policy Acknowledgment Form.
Contractors and affiliated entities will be required to acknowledge this policy as part of their contract, service or affiliation agreement.

Contact:

Information Technology Division

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **15 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

LINKS TO SUPPORTING DOCUMENTS

1. IT Use Policy Acknowledgement Form
2. IT Security Governing Principles
3. Care, Custody and Control of City Assets Policy
4. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
5. Canada's Anti-Spam Legislation, s.c. 2010, c.23
6. Secure Electronic Signature Regulation of Canada
7. Workplace Harassment Prevention
8. Employee Code of Conduct
9. Code of Conduct for Members of Council
10. City's Information Management Policy
11. Personal Information Protection Policy
12. Records Retention By-law 163-2008
13. Purchasing By-law
14. Purchasing Card Policy
15. SOP for the Use of Social Media for Business Purposes
16. BYOD Program
17. Privacy Statement
18. Corporate Printing Governing Principles
19. IT Managed Services, Service & Operational Level Agreement (SOLA)
20. IT Architectural Controls and Standards
21. CoB Technology Environment Architectural Standards
22. IT Project Management Governing Principles
23. IT Service and Standards Catalogue

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **16 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

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.
Electronic & Digital Signature	A technology based encryption key associated with a digital certificate issued by a trusted and reputable certificate authority and can be associated with a styled signature captured by a Signature Pad or image capturing tools.
Information Assets	Including but not limited to data/software and/or electronic documents, electronic signature and communication written and/or developed by Users related to their work at the City.
Information and Communication Technology (ICT)	Computers, systems, mobile communication devices, electronic communication, telephones, servers, applications, data, software tools, electronic access accounts, information assets, technology acquisition,

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **17 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

Term	**Meaning**
	technology standards and processes, network resources and the overall Business-Technologies and Infrastructure
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.
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 Information Technology Use Policy or IT Security Governing Principles
Signature Pad	A technology devise that captures an individual signature via a stylist or electronic pen.

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **18 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

Term	**Meaning**
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	Spam generally refers to the use of electronic messaging systems to send unsolicited, bulk messages. Spam messages may contain deceptive content, support illegal activities and may also be used to deliver electronic threats such as spyware and viruses.
Commercial Electronic Message (CEM)	*Any electronic message that encourages participation in a commercial activity, regardless of whether there is an expectation of profit*
User or Users	All and any persons or entities that have access to and/or make use of the City's ICT in any form or plan except anonymous persons (e.g. people surfing the City's public website)
Bring Your Own Device	Personally owned mobile communications devices that are being used by employees and other personnel for work related purposes to access one or more corporate resources such as Email or the Internet. They are

SECTION: **CORPORATE SERVICES** SUBJECT: **INFORMATION TECHNOLOGY (IT) USE POLICY**		POLICY NO.: **2.11.0**
EFFECTIVE: **OCTOBER 1, 2014** **(WITH 90 DAYS TRANSITION PERIOD)**	REPLACES: **2.11.0 IT USE POLICY** **APPROVED MARCH 17, 2011**	PAGE: **19 of 19**
APPROVED BY: **COUNCIL, RESOLUTION C266-2014** **APPROVED SEPTEMBER 10, 2014**	PROCEDURAL UPDATES: **IT Security Governing Principles** **IT Use Policy Acknowledgement Form**	

Term	**Meaning**
	typically mobile devices such as wireless smart phones and tablets.
Mobile Communications Device (s)* or Mobile Device	The term “mobile communications device” may include but is not limited to: Netbooks, Mobile Smart Device, Slates, Tablets, Mobile/cellular phones, Smartphones, and Personal digital assistants (PDAs).