	HUMAN RESOURCES AND CITIZEN SERVICE POLICIES	Section # I	Policy # 6
		Approval Date: Sept 2006	Revision Date: Feb 2013
Title:	**USE OF INFORMATION TECHNOLOGY**		
Applies To:	All Employees		

POLICY STATEMENT:

The purpose of the Region's Information Technology is to service the business requirements of the Region. All employees are required to use such Information Technology in a professional, ethical manner and in accordance with applicable legislation and policy, including safeguarding devices, data and information. The Region will monitor Information Technology to ensure appropriate use.

OPERATING DETAILS:

Information Technology is provided and intended to be used primarily for the Region's business purposes. Accordingly, use must relate to the work of employees and to the fulfillment of their administrative and operational functions and responsibilities. Employees who are found to be using the Region's Information Technology for unacceptable uses may be subject to discipline up to and including dismissal.

MONITORING USE OF INFORMATION TECHNOLOGY

The Region reserves the right to monitor Information Technology belonging to the Region, to ensure appropriate use. Employees should have no expectation of privacy as it relates to their use of Regional Information Technology. If an employee requires a private means of computing and/or communicating, they must use a personal device unconnected to the Region's network. Use of personal communication devices should be limited to breaks and lunches.

The Region reserves the right to monitor and review any Information Technology use in order to:

1. Ensure compliance with this and other Regional policies;
2. Ensure the continued operation of IT systems;
3. Access business-related information when an employee is absent;
4. Access information for any other purposes deemed legitimate by the Region which include but are not limited to: business purposes, legal compliance, human resources or corporate purposes, defending litigation, or responding to MFIPPA or PHIPA access requests.

The Region monitors Information Technology through means such as activity logs, performance and threat reports and content analysis utilities including, but not limited to:

- User account activity logs,

- Network traffic activity logs and performance reports,
- User virtual private network logs, end point compliance and performance,
- Email filters and performance,
- Internet Usage logs,
- Corporate or critical applications and databases activity, and
- Storage including network and personal drives.

Employees may generate information when using IT systems, such as activity log files and "deleted" information not viewable by the user.

It is recognized that employees may occasionally need to access IT systems for personal use. Such use is permitted provided that it is limited, occasional, and does not in any way interfere with the employee's work performance or with any other employee's ability to fulfill their administrative and operational functions or responsibilities, or incur financial loss for the Region.

For examples of acceptable and unacceptable use of information technology, please refer to Appendix A.

ACCESS CONTROL

All Information Technology devices, including laptops, tablets, and smartphones (BlackBerry), used for Region business must be password protected when inactive and/or unattended. Users shall not share account or password information with another person. Passwords, if documented, should be secured appropriately. Users must take all necessary precautions to prevent unauthorized access to the Region's Information Technology.

The primary purpose of a password is to authenticate or identify users, and is not intended to restrict management or Information Technology Services Employee's access.

The authority to permit third party access (i.e. access by a party other than the Region) rests with the Director, Information Technology Systems. Where such access is related to IT systems and applications other than those owned by the Region, consultation will take place with an appropriate member of senior management from the department involved.

PHYSICAL SECURITY OF INFORMATION TECHNOLOGY

Management and employees are responsible for the physical security of Information Technology devices and must keep them in a secure place. Department management is responsible for ensuring that only authorized employees have access to Information Technology in their possession. Any employee who suspects an Information Technology device is lost or stolen must immediately report it to their supervisor and/or other management, and the ITS service desk. Any expense associated with the loss of the device is the financial responsibility of the department.

All Regionally owned Information Technology devices that are temporarily loaned or assigned to employees must be kept in a secure location at all times, booked or reserved for the period of use, and accessed through a formalized sign out/sign in procedure.

PRIVACY CONSIDERATIONS

Use of Information Technology must comply with all applicable legislated and corporate privacy standards such as the *Personal Health Information Protection Act,* and the *Municipal Freedom of Information and Protection of Privacy Act*. Direction can be obtained from immediate managers and/or the Information Access and Privacy Advisor.

DATA PROTECTION

Personal Health Information and Personal Information that requires being transported on any mobile device(s) or accessed externally via web must be encrypted using a Regionally approved encryption solution which meets the *Federal Information Processing Standards* (FIPS), currently FIPS 140-2.

It is the relevant management staff's and employee's responsibility to determine whether encryption is required. The employee may consult with Information Management and Archives, the Information Access and Privacy Advisor, and\or ITS to assist in this determination.

SECURITY INCIDENT

Any employee who discovers or suspects a Technology Security Incident must immediately report it to their supervisor and/or other management, and the ITS service desk.

RECORDS RETENTION

Retention of electronic records including Electronic Messaging is subject to the *Information Retention and Disposal Schedule*, By-law 93-076.

A record may be in different forms including but not limited to paper, electronic or audio visual. All business-related records are governed by Regional retention practices. Transitory records can be destroyed at the employee's discretion. Because of the nature of the technology, text messages, BlackBerry Messenger and other forms of pin-to-pin communications should only be used for transitory purposes and/or when normal communication channels are unavailable.

DEFINITIONS:

Information Technology (IT) means: all electronic data processing, storage and electronic communication devices used by the Region which include but are not limited to all computer and telephone networks and applications, tablets, smartphones (e.g. BlackBerry), mobile/ cell phone, pager, and portable data storage device (e.g. USB drive). It includes all hardware (tangible physical components) and all software (computer programs and related data).

Electronic Messaging means: any correspondence that is transcribed through the use of messaging technology. This includes, but is not limited to, e-mail, instant text messaging, BlackBerry Messenger and other forms of pin-to-pin communications, chat programs, and third party hosted solutions.

Personal Health Information (PHI) means: information that is about a directly or indirectly identifiable individual, and which relates to:

- The individual's physical or mental health;
- The provision of health care to the individual, and
- Associated health care information such as Health Card Number or eligibility for a health care service.

Personal Information (PI) means: information about a directly or indirectly identifiable individual. Personal Information includes, but is not limited to:

- Any contact or location information;
- Information that describes an individual's involvement with Regional services;
- An individual's financial, employment or educational histories;
- Identification numbers, and
- Personal opinions or correspondence.

Encryption means: the process of transforming plaintext using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually a key.

A Technology Security Incident means: an activity which results (or may result) in a loss or theft of digital information or IT equipment/devices, unauthorized access, malicious code, a hack and/or a virus.

Transitory records means: records of temporary usefulness that have not recorded an official business decision or do not have legal, financial, operational and official requirements.

SEE ALSO:

- Applicable Privacy Legislation, including MFIPPA and PHIPA
- Code of Ethics and Conflict of Interest (I-8) DOCS #41840
- Confidential Information (I-4) Docs #41657
- Corporate Resources ITS Procedures, Section 5 (Available in the Policies and Procedures section of the employee portal)
- Disciplinary Action (I-28) Docs #41684
- E-Mail Management Guideline Docs #687942
- Interpersonal Conduct (I-14) Docs #41664
- Political Candidacy and Campaign Activities (I-2) Docs #41655
- Protection of Proprietary Information (I-29) Docs #41686
- Public Criticism of Employer (I-31) Docs# 41688
- Use of Regional Equipment & Vehicles (I-27) Docs #41683
- Regional Social Media Sites (I-38) Docs #647322
- Workplace Harassment (I-14) Docs #41664
- Workplace Violence Prevention (IV-15) Docs #41779

FOR FURTHER INFORMATION PLEASE CONTACT:

- Director, Information Technology Services,
  Corporate Resources

- Director, Employee Relations,
  Human Resources and Citizen Service

- Information Access and Privacy Advisor,
  Council and Administrative Services Division,
  Corporate Resources

- Manager, Information Management and Archives,
  Council and Administrative Services Division,
  Corporate Resources

ACCEPTABLE USE:

Examples of acceptable use of information technology include:

1. Communicating with fellow employees, business partners of the Region and clients within the context of an individual's assigned responsibilities;
2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and
3. Participating in educational or professional development activities.

Uses relating to Regionally approved events, announcements, or extra-curricular activities, (e.g. Sunnyside Walk/Roll, United Way, baseball teams, retirement functions, authorized employee announcements) are considered to be for business purposes.

UNACCEPTABLE USE:

Examples of unacceptable uses include, but are not limited to:

- Personal use that is not limited and occasional;
- Personal use that interferes in any way with the performance of job duties of the employee or of any other employee;
- Uses that violate federal or provincial legislation including the Canadian Charter of Rights and Freedoms, the Canadian Human Rights Act, and the Ontario Human Rights Code;
- Illegal or unlawful purposes, including, but not limited to copyright, infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, gambling, soliciting for pyramid schemes, and computer tampering (e.g. spreading computer viruses);
- Uses that violate any other Regional policy including Workplace Harassment, Workplace Violence Prevention, Interpersonal Conduct, Code of Ethics and Conflict of Interest, Confidential Information, or Public Criticism of Employer;
- Accessing, storage, display, creation, exchange, transmission, or downloading of messages or other data that are harassing, discriminatory, offensive, libellous, demeaning, insulting, abusive or threatening to any other party. The term "other party"

includes, but is not limited to, any other employee of the Region and the Region itself;

- Downloading, viewing, or in any way collecting or accessing pornographic material, violent material, or hate literature of any kind;

- Uses that could result in damage to the Region's reputation or result in the Region incurring unauthorized costs;

- Solicitation in relation to any personal ventures (including business, political, charitable, or religious ventures) which are unrelated to the Region's business purposes;

- Election-related purposes, as defined in HR Policy I-02, Political Candidacy and Campaign Activities;

- Any union business except where express permission has been granted by the Employee Relations Division of Human Resources;

- Attempts to destroy or manipulate data or otherwise sabotage electronic systems or information, including disseminating or facilitating the dissemination of malware such as viruses, worms, adware etc.;

- Gaining or attempting to gain unauthorized access to information;

- Misappropriation (using for other purposes than intended or for purposes that are not related to an employee's job) of software and or data that could result in litigation;

- Use for mass unsolicited mailings for unapproved purposes;

- Allowing unauthorized non-employees to use or access Regional resources or network facilities; and

- Uploading and downloading of files for personal use.