THE CORPORATION OF THE CITY OF WINDSOR
POLICY

Service Area:	**Office of the City Treasurer**	Policy #:	
Department:	**Information Technology**	Approval Date:	**September 18, 2017**
Division:		Approved By:	**CR 554/2017**
		Effective Date:	**September 18, 2017**
		Procedure Ref.	
Subject:	**ACCEPTABLE USE POLICY**	*Pages:*	
Review Date:	**September 2020**		Replaces: M109/2013
			Date: February 14, 2013

1. POLICY

1.1 The Acceptable Use Policy identifies roles, responsibilities, and requirements for the appropriate use of Corporate Technology Resources.

1.2 Authorized Users are granted permission to use data, systems, and technologies that belong to the Corporation in accordance with the Acceptable Use Policy.

1.3 Failure to conform to the requirements of This Policy may result in disciplinary action up to and including termination, legal action, and/or possible criminal proceedings.

2. PURPOSE

2.1 The goal of This Policy is to protect The Corporation of the City of Windsor from legal liability and to reduce the risk of damage, loss, or theft to Corporate Technology Resources. The following additional goals are specific to the technologies listed:

2.1.1 **Corporate Data:** To protect the integrity of Corporate electronic data, and to safeguard it from unauthorized access, damage, loss, theft, or unauthorized disclosure.

2.1.2 **Software Licensing/Copyright:** To ensure legal compliance with licensing agreements for software and copyright laws for electronic data files, and to ensure that legal compliance with proper process is approved throughout the Corporation.

2.1.3 **Corporate Hardware:** To ensure that Corporate Hardware and Corporate Communication Systems are used for business purposes, and to eliminate damage, loss, and theft of the Hardware / Communication Systems.

2.1.4 **Passwords/Certificates:** To protect and safeguard Corporate resources, and to uniquely identify a User.

2.1.5 **Internet Access:** To ensure proper usage and availability of the Internet, and to protect Corporate resources from external Internet threats.

2.1.6 Electronic Mail: To define responsibilities with regard to privacy and appropriate use of electronic mail.

2.1.7 Corporate Telephones and Telephone Systems: To define responsibilities with regard to the appropriate use of Corporate Telephones and Telephone systems.

3. SCOPE

3.1 This Policy applies to the following Users of Technology Resources owned, leased, hosted by a 3rd party technology entity or licensed to the Corporation:

- Employees
- Management
- The Mayor and City Council
- Members of agencies, boards, and commissions that use Corporate Technology Resources
- Any individual retained by the Corporation who uses the Corporation's Technology Resources

4. RESPONSIBILITY

4.1 The following parties, as identified in Section 3.1 and described under Section 5.2 of This Policy are responsible for the various aspects of This Policy:

- Users
- Management
- Security Administrator
- System Administrators
- Technology Group Leaders
- Executive Director of Information Technology

4.2 The general responsibilities of each of the parties identified in Section 4.1 is detailed with duties pertaining to specific technologies defined in Section 5:

4.2.1 Each **User** has the following responsibilities:

4.2.1.1 Understand, accept, and abide by This Policy including its Governing Rules and Regulations and associated procedures.

4.2.1.2 Use the Corporate Technology Resources for business purposes that benefit the Corporation and are directly applicable to his/her job.

4.2.1.3 Ensure use of the Corporate Technology Resources conforms to This Policy and any other Corporate policies, codes of conduct, Corporate health and safety standards, and any related legislation.

4.2.1.4 Know that suspected infractions of This Policy may be reported to his/her immediate supervisor or to the Concerned Citizen/Concerned Employee Hotline.

4.2.1.5 Know that any person who witnesses, or is the recipient of Child Pornography, on any Corporate Technology Resource, is legally bound by the *Child and Family Services Act*, to report it to his/her immediate supervisor or the Concerned Citizen/Concerned Employee Hotline.

4.2.1.6 Know that the identity of an individual who reports a suspected infraction concerning Child Pornography is protected under the *Child and Family Services Act*.

4.2.2 **Management** has the following responsibilities:

4.2.2.1 Abide by the responsibilities of a User.

4.2.2.2 Ensure staff are aware of and have attended training for This Policy.

4.2.2.3 Ensure any changes or amendments to This Policy are adequately communicated to and understood by supervised staff.

4.2.2.4 Authorize the access of supervised staff to Technology Resources that falls under their responsibility.

4.2.2.5 Ensure that any policy exception requests or Technology Resource access changes for supervised staff members follow the Corporate technology procedures.

4.2.2.6 Report any suspected infraction of This Policy to the Executive Director of Information Technology.

4.2.2.7 Notify the Executive Director of Human Resources immediately, and the appropriate Executive Director, if applicable, if any disciplinary action is intended or suspected as a result of an infraction of This Policy.

4.2.2.8 Track their employees' infractions of This Policy as well as the resulting corrective actions, recommendations, and referrals.

4.2.2.9 Work with Information Technology when acquiring any technology for the Corporation, as per the Corporation's Purchasing By-law and Information Technology's Project Management Policy.

4.2.3 The **Security Administrator** has the following responsibilities:

4.2.3.1 Abide by the responsibilities of a User.

4.2.3.2 Review, recommend, and implement changes to This Policy and its associated procedures.

4.2.3.3 Audit the Technology Resources to ensure compliance with established policies and procedures, and work with the Executive Director of Information Technology to accommodate Audit requirements.

4.2.3.4 Act as a liaison with Management and System Administrators throughout the Corporation regarding security-related issues occurring with information and Technology Resources.

4.2.3.5 Investigate any reported infractions of This Policy. In the case of suspected criminal activity the investigation will be the responsibility of law enforcement.

4.2.4 **System Administrators** have the following responsibilities:

4.2.4.1 Abide by the responsibilities of a User.

4.2.4.2 Implement This Policy and its associated procedures on the Technology Resources they are authorized to administer.

4.2.4.3 Audit Technology Resources for compliance to This Policy and its associated procedures.

4.2.4.4 Track and approve requests for adds/removes/changes and policy exceptions for Technology Resources they administer.

4.2.5 **Technology Group Leaders** have the following responsibilities:

4.2.5.1 Abide by the responsibilities of a User.

4.2.5.2 Be up-to-date with Information Technology policies, standards, and procedures.

4.2.5.3 Provide local assistance to staff for designated responsibilities defined in the Information Technology procedures.

4.2.5.4 Liase with Information Technology with regard to Corporate technology issues for their area of responsibility.

4.2.6 **The Executive Director of Information Technology** and his/her appointed designate(s) have the following responsibilities:

4.2.6.1 Establish procedures and standards related to This Policy to ensure the Corporation's technology systems are running in an efficient and optimal manner (e.g. setting system maintenance schedules, and data archiving).

4.2.6.2 Provide Users access to all Information Technology policies and procedures.

4.2.6.3 Provide education and address any concerns the User may have as to his/her responsibilities under This Policy.

4.2.6.4 Access the Corporation's Technology Resources for the purposes of Auditting, investigations, conducting e-discovery, performance analysis, backup, filtering, and work continuity.

4.2.6.5 Conduct monitoring, reproduction of deleted data, review of current and archived data, and User activity of the Corporation's Technology Resources according to established policies and procedures.

4.2.6.6 Establish related procedures for the acquisition and justification of Hardware, software, and Technology Resources.

4.2.6.7 Issue Corporate-wide emails pertaining to system maintenance and technology-related bulletins (e.g. virus alerts).

4.2.6.8 Be responsible for records produced pertaining to and including This Policy, and do the following:

4.2.6.8.1 Maintain standards and policies for Corporate technology acquisition and use within the Corporation, with advice from City departments, as per Purchasing By-law 93-2012.

4.2.6.8.2 Review This Policy at least once during each term of City Council.

4.2.6.8.3 Develop and maintain Corporate approval forms relating to the request for access, acquisition, relocation, and removal of Corporate Technology Resources.

4.2.6.8.4 Track the requests for access, acquisition, relocation, and removal of Corporate Technology Resources to ensure accurate and up-to-date inventory records and security requirements.

4.2.6.9 Recommend adequate security measures for Technology Resources.

4.2.6.10 Be responsible in the case of a suspected criminal activity violation to report it to, and take direction from, the City Solicitor.

5. GOVERNING RULES AND REGULATIONS

5.1 The processes required to attain the policy goals, including jurisdiction and control requirements, include the following:

5.1.1 User Duties: Users shall do the following for the Technology Resources noted below:

5.1.1.1 Corporate Data:

5.1.1.1.1 Ensure the Corporate data for which he/she is responsible is accurate and up-to-date and that he/she does not knowingly enter invalid data.

5.1.1.1.2 Ensure he/she does not use, copy, or distribute Corporate data for any purpose other than for the business purposes of the Corporation.

5.1.1.1.3 Know the disclosure level for Corporate data according to Corporate policy and legislative acts as listed under Section 6.

5.1.1.1.4 Ensure that the data for which he/she is responsible is stored in the assigned secure location. This includes the requirement to <u>not</u> store Corporate data, even temporarily, on devices or with services that are not sanctioned by the Corporation's Information Technology Department. In extenuating circumstances, employees may use personal or non-Corporate devices or services to store Corporate data as long as the following conditions are met:

- The employee has obtained the approval of his/her manager prior to storing the data on the personal or non-Corporate device or service;
- A copy of the data is stored in the appropriate Corporate system, ensuring that the Corporation's information is protected; and
- The data is immediately deleted from the personal or non-Corporate device or service as soon as possible after dealing with the extenuating circumstance.

Employees should know that they could be held responsible if Corporate information should be lost or exposed due to the use of their personal or non-Corporate devices or services.

5.1.1.1.5 Know that User access controls, created by Users or otherwise, to resource secure locations are for the benefit of the Corporation and not to be considered private by the User.

5.1.1.1.6 Contact the Corporation's Information Technology Department to arrange for the back-up of Corporate data that is not currently stored on the Corporate network.

5.1.1.1.7 Archive data in a suitable and secure location and/or removable media if the maintenance schedule for the system in which the data currently resides is shorter than the requirements of the Corporation's Records Retention By-law Number 21-2013.

5.1.1.1.8 Remove personal data and non-essential duplicate data from Corporate Technology Resources to conserve storage and ensure systems run optimally.

5.1.1.2 Software Licensing/Copyright:

5.1.1.2.1 Shall not download, copy, or install any software for which the Corporation does not have a software license agreement and Information Technology approval was not obtained.

5.1.1.2.2 Shall not download, copy, or install any electronic data files, e.g. music, movies, or ebooks, that violate copyright laws, or violate any existing software licensing agreements.

5.1.1.2.3 Notify Information Technology if he/she notices any illegal software or electronic data files on any Corporate resource.

5.1.1.2.4 Coordinate with Information Technology to download, copy, or install approved software or electronic data files.

5.1.1.3 Corporate Hardware:

5.1.1.3.1 Use Corporate Hardware and Corporate Communication Systems for the Corporation's business purposes.

5.1.1.3.2 Shall not move Corporate Hardware or Corporate Communication Systems that are designated to be stationary (e.g. PCs, desk Phones, printers) without consent from Information Technology.

5.1.1.3.3 Ensure that his/her Corporate Hardware, including laptops, handhelds, smartphones, are protected and secure from theft, loss, or damage.

5.1.1.3.4 Ensure his/her Corporate Hardware is screen locked, i.e. Password-protected, when leaving the system unattended.

5.1.1.3.5 Know that mobile Corporate Hardware, i.e. laptops, handhelds, tablets, smartphones, etc., are considered Corporate Technology Resources and issued for work purposes even though they may periodically be used as stand alone devices.

5.1.1.3.6 Return all his/her assigned Corporate Hardware to his/her supervisor upon termination of employment or when job duties no longer require use of the Hardware.

5.1.1.3.7 Know that only Information Technology staff are authorized to alter, modify or dismantle Corporate Hardware or Corporate Communication Systems.

5.1.1.4 Passwords/Certificates:

5.1.1.4.1 Keep Passwords private and secure. Users are fully responsible for all activities invoked through their Userid and Password.

5.1.1.4.2 Know that an assigned Userid and Password does not constitute User privacy, but is for the purpose of User authentication and authorization and does not preclude Corporate access.

5.1.1.4.3 Change Passwords whenever they are suspected of no longer being private and secure.

5.1.1.4.4 Use Information Technology's Password procedure for the resetting or assigning of new Passwords.

5.1.1.4.5 Ensure that the Password complexity selected is at an acceptable security level.

5.1.1.4.6 Assigned certificates should be treated as Passwords and kept private and secure.

5.1.1.5 Internet Access: Ensure proper usage of the Internet. Proper usage includes, but is not limited to, the following:

5.1.1.5.1 Networking with colleagues, the private sector, industry, and professional associations.

5.1.1.5.2 Researching and sharing authorized information.

5.1.1.5.3 Monitoring the latest news and trends as it pertains to the User's job function.

5.1.1.5.4 Conducting Corporate business.

5.1.1.6 Electronic Mail:

5.1.1.6.1 Know that electronic mail messages are considered Corporate data, and that Users should have no expectation of privacy in their electronic mail messages sent or received.

5.1.1.6.2 Maintain the confidentiality of electronic mail messages except where disclosure is required by law or in accordance with Corporate policy.

5.1.1.6.3 Use electronic mail for the Corporation's business purposes.

5.1.1.6.4 Use his/her Corporate e-mail account when conducting the Corporation's business; this includes while working outside the workplace. In extenuating circumstances, employees may use their personal or other non-Corporate e-mail account as long as the following conditions are met:

- A copy of the e-mail is sent to their Corporate e-mail account, ensuring that the Corporation's information is stored in a protected Corporate system;
- The e-mail is immediately deleted from their personal or non-Corporate e-mail account as soon as possible after dealing with the extenuating circumstance; and
- The amount of confidential information collected, accessed, used, or disclosed is limited to the least amount necessary to deal with the extenuating circumstance.

Employees should know that they could be held responsible if Corporate information should be lost or exposed due to the use of their personal or non-Corporate e-mail account.

5.1.1.6.5 Know that any department other than the Mayor's Office, Chief Administrative Officer's Office, or Corporate Communications shall obtain permission to send Corporate-wide electronic mail prior to sending.

5.1.1.7 Corporate Telephones and Telephone Systems:

5.1.1.7.1 Use Corporate Telephones and voice mail for Corporate business purposes. Reasonable personal calls are permitted if they fall within the duration and time periods acceptable to an individual's supervisor and do not violate any other sections of This Policy, or any other Corporate policy. Personal Telephone use is not permitted if there is a cost to the Corporation (e.g. long distance, toll numbers, unreasonable time lost, etc); however, it is recognized that there may be a rare occasion where a personal long distance call is necessary. If a personal long distance call is

required, permission must be obtained from the individual's supervisor prior to making the call.

5.1.1.7.2 Know and follow the voice mail procedures for the voice mail system(s) on his/her Corporate Telephone(s).

5.1.1.7.3 Maintain the confidentiality of voice mail messages except where disclosure is required by law or in accordance with Corporate policy.

5.1.1.7.4 Report unusual occurrences with his/her voice mail, such as frequent hang-ups, off work-hour activity, and suspicion of Password tampering.

5.1.1.7.5 Know that Telephone calls and voice mail messages may be monitored and as such, there should be no expectation of privacy.

5.1.1.7.6 For those employees who have access to televisions, it is unacceptable for employees to view sexually explicit programming or programming that contains material of a discriminatory or harassing nature.

5.1.2 Management Duties: In addition to abiding by User duties, Management also shall do the following for the Technology Resources noted below:

5.1.2.1 Corporate Data:

5.1.2.1.1 Review their staff requests to use personal or non-Corporate devices or services for transmitting and/or storing Corporate data. Management should know that they could be held responsible if Corporate information should be lost or exposed due to their staff's use of personal or non-Corporate devices or services.

5.1.2.1.2 Grant and revoke access rights for departmental data and applications.

5.1.2.1.3 Submit their employees' permission requests for Corporate electronic data (i.e. for the granting, revoking, and maintaining of same).

5.1.2.1.4 Notify Information Technology if a User requires temporary access rights to Corporate electronic data.

5.1.2.1.5 Ensure that their staff who enter data into Corporate systems have received the appropriate training and are aware of the rules for entering data into those systems.

5.1.2.2 Corporate Hardware:

5.1.2.2.1 Submit a request to Information Technology if Hardware or software needs to be moved, added, or replaced.

5.1.2.2.2 Notify Information Technology immediately if departmental staff members have added, removed, or moved equipment so Corporate inventory records may be kept up-to-date.

5.1.2.2.3 Obtain Corporate Hardware from supervised employees when the employee has been terminated or the Hardware is no longer required for his/her job function.

5.1.2.2.4 Work with Information Technology to protect and secure Corporate Hardware that is accessible by the public.

5.1.3 Policy Violations: Any individual who willfully or purposefully does not abide by the sections pertaining to him/her is considered to be in violation of This Policy. Additionally, using any Corporate technology for the following purposes is considered a violation of This Policy:

5.1.3.1 Compromising the security of Corporate Technology Resources.

5.1.3.2 Soliciting for personal business reasons, promoting personal causes or associations, or advertising the sale of any item. The Corporate bulletin boards (electronic or otherwise) are available for these purposes, but any postings shall conform to This Policy and any other Corporate policies.

5.1.3.3 Using Internet Access or electronic mail to visit sites, download, solicit, or disseminate materials that are offensive and/or threatening, pornographic in nature, contain hate propaganda, or other disparagement towards others based on their race, ethnicity, sex, sexual orientation, age, disability, and religious or political beliefs.

5.1.3.4 Concealing or misrepresenting, or so attempting to do, the origin of any communication of a malicious nature initiated by the sender or forwarded.

5.1.3.5 Using system resources for the storage of non-business related data or information (e.g. personal photos, desktop wallpaper, games, music).

5.1.3.6 Degrading system performance such as reducing available bandwidth for others through non-business use of Internet and network resources.

5.1.3.7 Representing oneself as someone else through the use or misuse of technology.

5.1.3.8 Participating in frivolous communications.

5.1.3.9 Violation of any of the Corporation's policies, By-laws, employee codes and standards of conduct, such as, but not limited to the Standards of Employee Deportment, Workplace Violence Prevention Policy, and the Respectful Workplace Policy.

5.1.3.10 Violations of any provincial or federal legislation or regulations.

5.1.4 Corporate Authority: The following describes the methods available to the Corporation for regulating compliance of This Policy:

5.1.4.1 The Corporation reserves the right to use technology systems, activity logs, performance analyzers, data recovery and archival tools, monitoring and filtering tools, and visual confirmation as a means of tracking and documenting violations of This Policy.

5.1.4.2 The Corporation reserves the right to view and access data on Corporate systems even if they are marked or flagged as "personal". This includes, but not limited to the use of forensic tools to retieve deleted information, or access information from Corporate systems that cannot be readily seen, e.g. log files.

5.1.4.3 The Corporation reserves the right to delete or archive, personal or non-essential data or files on Corporate resources.

5.1.4.4 Appropriate disciplinary action will be taken in accordance with the severity and frequency of the violation to This Policy. This discipline could include removing access to the Technology Resource, a verbal or written warning, a suspension, termination of employment, and/or billing the employee for misuse of the technology.

5.1.4.5 The Corporation reserves the right to enlist law enforcement officers or bring legal action against a violator according to the severity of the breach of compliance with the policy.

5.1.4.6 The Corporation will exercise discretion on instances where the policy violation was unsolicited by the User.

5.1.5 Policy Exceptions, Clarifications, and Formal Challenges: A User making a policy exception request shall follow proper process by making the request to his/her immediate supervisor. Likewise, a User may request a clarification of This Policy or its related procedures at any time and shall follow proper process by making the request to his/her immediate supervisor. If necessary, the supervisor will bring the request forward.

5.1.6 Personal Use of Corporate Technology: Notwithstanding the foregoing regulations, limited personal use may be permitted where such use does not:

- increase costs
- reduce productivity
- impact network performance

- interfere with work duties
- limit accessibility of shared Corporate technology
- violate This Policy
- impact negatively on the Corporation's reputation

Data or information created or stored using the Corporation's electronic media is not private and may be monitored or tracked by the Corporation at any time without notice. If a confidential means of sending and recieving personal communications and storing of personal files are required, use a personal device unconnected to any Corporate Technology Resource.

5.2 Definitions:

5.2.1 **"Audit"** means to engage a Technology Resource in e-discovery for the purposes of legal requirements; ensure continuity of work processes; to improve business processes and manage productivity; and to prevent misconduct and ensure compliance with the law.

5.2.2 **"Child Pornography"** is defined as stated in the *Child and Family Services Act* of Ontario.

5.2.3 **"Communication Systems"** include, but are not limited to, the following:

- E-mail
- Phones (including cell Phones)
- Voice mail
- Faxes
- Internet communication services (such as instant messaging, SMS, blogs, forums, social-networking, etc.)

5.2.4 **"Corporate"** means of or pertaining to the Corporation.

5.2.5 **"Corporation"** refers to The Corporation of the City of Windsor.

5.2.6 **"Hardware"** includes, but is not limited, to the following:

- Desktop computers
- Laptops
- Notebooks
- Handheld computers (including personal information devices)
- Printers
- Modems
- Cables
- CD's (i.e. compact disks)
- Floppy disks (i.e. floppies)
- Electronic devices connected to Corporate assets
- Peripherals
- Wireless devices

5.2.7 **"Internet Access"** includes Instant Messenger and other Internet services.

5.2.8 **"Legally Owned Software"** is software for which proof of legal ownership can be produced. If the proof cannot be produced, then it is considered to be illegal. Any of the following can serve as proof of ownership:

- The original license for the software package.
- A purchase order for the software package.
- A cheque request for the software package.
- An original disk/cd with a serial number for the software package.
- Proof of purchase from the vendor.
- Vendor documentation for freeware/free downloads.

5.2.9 **"Management"** is defined as non-union staff members with direct reports.

5.2.10 **"Password"** includes Personal Identification Numbers, pass phrases, and two-factor authentication devices. A digital **certificate** is another mechanism that can identify a specific User or device.

5.2.11 "P**hones"** and "T**elephones"** includes cell Phones, desk Phones, fax machines, and the voice option on BlackBerrys.

5.2.12 **"Security Administrator"** is the designated staff person who is responsible for the security of information and information technology. In some situations, this function may be combined with the System Administrator.

5.2.13 **"System Administrator"** is the designated staff person who is responsible for the day-to-day operation of system and network resources.

5.2.14 **"Technology Group Leader"** is the designated staff person who will assist assigned work area staff with technology policy and procedure issues and questions, as well as act as a liaison with Information Technology to ensure technology procedures are being followed. This function is performed by the Managers of Administration for the department; however, depending on the departmental structure, this role could be filled by different staff (e.g. Phone book editors, Internet/Intranet web content editors).

5.2.15 **"Technology Resources"** include, but are not limited to, data, software, Hardware, telecommunications, and networking.

5.2.16 **"This Policy"** is defined as the Acceptable Use Policy and its associated procedures.

5.2.17 "**User"** is defined as an employee, student, intern, volunteer, councillor, Mayor or board member of the City of Windsor or its agencies who uses Corporate Technology Resources, whether explicitly or implicitly, by signing on or using a system.

5.2.18 **"Userid"** is a unique individual identification protected by a Password, or other secure authentication method, to gain access to Corporate and departmental systems, resources and applications, for example voice mail.

6. RECORDS AND REFERENCES

6.1 Documents generated as a result of This Policy will be maintained in accordance with the Corporation's Records Retention By-Law 21-2013.

6.2 The following Information Technology procedures and forms are related to This Policy and are located on the Corporate Intranet:

- Exception Request procedure
- User Add/Change/Delete Access procedure
- Hardware, Software, or System Acquisition and Justification procedure.
- Relocation and/or Removal of Corporate Hardware, Software, Data, or Systems procedure.
- Telephone and Telephone System procedures
- Password procedure
- Archiving of Corporate Data and E-mail procedure
- Out-of-Office procedure for Voice Mail and E-mail

6.3 **Referenced Policies:** The Acceptable Use Policy is intended to support and augment the following policies and legislation, or their latest revision, dealing with similar or related issues:

- Code of Ethics and Conflict of Interest for Staff and Volunteers Policy – M287/2015, July 20, 2015.
- Concerned Employee Policy – M140/2015, April 20, 2015.
- Records Retention By-law 21-2013.
- Code of Conduct for Members of Council and Boards and Committees – CR180/2011, June 7, 2011.
- Cellular Devices Policy – CR6/2015, January 5, 2015.
- Fraud and Misuse of Assets Policy – M140/2015, April 20, 2015.
- Social Media Policy – M247/2013, June 17, 2013.
- Standards of Employee Deportment – CR479/2006, October 2, 2006.
- Workplace Violence Policy - CR217/2010, June 7, 2010.
- Respectful Workplace Policy - CR746/2005, December 5, 2005.

- Project Management Methodology Policy - CR252/2014.
- The Province of Ontario's Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).
- The Federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CanSPAM).
- The Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
- Purchasing By-law 93-2012.
- Child and Family Services Act (C.11).
- Criminal Code (Canada).

If a conflict should arise between policies in the areas of interpretation, application, or responsibility, the policy with the more stringent or restrictive interpretation shall apply.