POLICY

	Policy:	**INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY**		
	Department:	Corporate Services		
	Division:	Information Technology	By-Law No.:	N/A
	Administered By:	Manager, Information Technology	Approval Date:	DRAFT
	Replaces:	*Technology Use Policy – February 6, 2012*		
	Attachment(s):	N/A		

1. POLICY STATEMENT

The Corporation of the Town of Amherstburg recognizes that access to technology is an essential element to the daily operations of Town business, and as such is committed to establishing procedures that define the acceptable use of the various Information Technology (IT) resources provided to users.

2. PURPOSE

2.1. This policy identifies authorized users' roles, responsibilities, and the requirements for the appropriate use of corporate technology resources.

2.2. This policy outlines the acceptable use of Information Technology resources and equipment such as the internet, electronic messaging, networks, computers, applications and mobile devices such as cell phones and tablets.

2.3. This policy ensures compliance with the Government of Ontario Information Technology Standards, Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and other legislative requirements.

2.4. This policy ensures the protection of the Town from legal liability and reduces the risk of virus attacks, compromise of network systems, damage, loss or theft of corporate technology resources and devices.

3. SCOPE

3.1. This policy applies to all users of technology resources provided by the Town of Amherstburg.

3.2. This policy shall be reviewed every five (5) years from the date it becomes effective, and/or sooner at the discretion of the CAO or designate.

4. DEFINITIONS

4.1. **Access** means permitted use of corporate information technology.

4.2. **Electronic Messaging** includes all forms of messaging, including the traditional Town Email system, and instant messaging applications.

4.3. **Firewall** is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. The Corporation uses a firewall to prevent unnecessary traffic from entering or exiting the

Corporation's network, for the goal of securing the Corporation's data and ability to do business.

4.4. **Information Technology** is any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

4.5. **Internet** is a global system of interconnected computer networks that use the standard internet protocol suite to serve users worldwide.

4.6. **Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)** provides individuals with a right of access to information under the control of institutions balanced with the right to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

4.7. **Password** refers to the individual personal password or security code assigned to the user's user ID, which may be updated by the user from time to time.

4.8. **Portable Storage Device** is a removable electronic device that has only memory and can copy and store data. PSDs may include memory sticks and cards, USB flash drives, portable hard drives, CDs, DVDs and disks.

4.9. **Social Media** refers to websites and other online means of communication that are used by large groups of people to share information and develop social and professional contacts.

4.10. **Social Networking** is the use of dedicated websites and applications to interact with other users, or to find people with similar interests to oneself.

4.11. **User** refers to any individual who uses Town computing and telecommunications facilities, including but not limited to Town elected officials, employees, volunteers, contractors, consultants and the public.

4.12. **Virtual Private Network** is a network that uses a public telecommunication infrastructure to connect remote offices or individuals user with secure access to the Corporation's network.

4.13. **Virus** is a piece of code that is capable of copying itself and typically has a detrimental effect such as corrupting the system or destroying data.

Common definitions, acronyms, and terms are available in the Glossary located on the Town's Policies webpage.

5. INTERPRETATIONS

Any reference in this policy to any statute or any section of a statute shall, unless expressly stated, be deemed to be reference to the statute as amended, restated or re-enacted from time to time. Any references to a by-law or Town policy shall be deemed to be a reference to the most recent passed policy or by-law and any replacements thereto.

6. GENERAL CONDITIONS

6.1. Account Activation/Termination

6.1.1. The level of access employees and members of council have to the Town's computers, networks, applications, internet services, email services and communication hardware is based upon specific job requirements.

6.1.2. Employees and members of Council must have approval of a department head and Corporate Services in order to gain access to the above technology. Without this approval, access shall not be granted.

6.1.3. All users are required to read this policy in accordance with the Corporation's Code of Conduct and sign the Code of Conduct Acknowledgement Form prior to receiving access rights and passwords.

6.1.4. Access will be terminated and any communication hardware shall be returned when the employee or member of Council terminates their employment with the Corporation, unless other approved arrangements are made.

6.2. General Security

6.2.1. The Corporation employs various measures to protect its equipment, systems and data from deliberate or inadvertent destruction or misuse. Such measures include:
- 6.2.1.1. Designation of individual accounts, log-ins, and passwords.
- 6.2.1.2. Security settings in software applications
- 6.2.1.3. Virus scanning software
- 6.2.1.4. Firewalls

6.2.2. Sharing of accounts, log-ins and passwords is prohibited unless an exception is granted by the Manager of Information Technology.

6.2.3. Employees and members of council shall not alter, or attempt to alter, any security setting or disable virus protection or attempt to bypass firewall protections without the approval of the Manager of Information Technology.

6.2.4. Electronic Devices that are not directly managed by the Information Technology division are not to be connected to the Corporations networks whether directly or via virtual private network or other remote access technologies.

6.3. Electronic Device Security

6.3.1. It is the responsibility of the employee or member of council to protect the confidentiality of their account and password information.

6.3.2. Each employee's or council member's password must be confidential, and in accordance with the Town's specific account security parameters.

6.3.3. In the event that a user, forgets, or believes that his or her password has become compromised, the user shall inform their Supervisor and the Manager of IT immediately.

6.4. Ownership

6.4.1. The Town strives to protect the confidentiality of all network users. However, all files and electronic communications, including email, internet and web content systems, created on, generated by or transmitted through the Town's computer and network services are deemed to be the property of the Town of Amherstburg.

6.4.2. The Town retains control, custody and supervision of all computers, networks, internet services, e-mail services and communication hardware usage. The Town reserves the right, at any time, to inspect and/or monitor system files, logs and other activities including electronic communication stored on any server or individual computer. The Town will uphold an electronic monitoring policy in compliance with provincial regulations under the Employment Standards Act.

6.4.3. Personal information that is stored on any Town device will not be considered private.

6.4.4. Upon cessation of employment for any reason, all personal information stored on the Town's systems or devices will be forfeited and will not be returned to the user.

6.5. Internet

6.5.1. Internet access is provided for work related activities and shall be used only in connection with an employee's or members of Council specific job duties. Permissible, acceptable, and appropriate Internet-related work activities include:

6.5.1.1. Researching, accumulating, and disseminating any information related to the user's assigned responsibilities.

6.5.1.2. Collaborating and communicating with other users, community/business partners, and customers of the Town, according to the user's assigned job duties and responsibilities.

6.5.1.3. Users shall not engage in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.

6.5.2. Only approved software or applications may be used in conjunction with activities on web browsers or platforms.

6.5.3. Employees and members of Council are encouraged to exercise care in selecting websites to visit on the internet, including sites received in, or linked from e-mail.

6.6. Electronic Communications

6.6.1. Electronic communication such as e-mail, social media, social networking, instant messaging helps facilitate business interactions at the Town, serving as a tool to support and enrich the exchange of information. All accounts must be approved by the appropriate Department Director and Director of Corporate Services and accessed using a program approved by the Manager of Information Technology.

6.6.2. Electronic communications may be considered public records under the Municipal Freedom of Information and Protection of Privacy Act. Employees and members of Council should assume that any electronic communication may be deemed "public information" and treated the same as any other written communication.

6.6.3. Use of personal email accounts is prohibited for work activities, excluding those activities explicitly outlined in the technology terms and provisions.

6.6.4. In no circumstances should electronic communications containing personal information be forwarded or copied to individuals outside the Corporation unless consent is provided for the disclosure in accordance with relevant legislation.

6.6.5. Employees and members of Council are cautioned to avoid using electronic communication mediums to promote, advocate or communicate personal views or the views of other individuals or organizations that could be perceived as an endorsement by the Corporation when no such endorsement has been provided.

6.7. Copyrights

6.7.1. The Town and its employees shall fully comply will all laws pertaining to the reproduction, use or distribution of copyrighted or otherwise protected materials.

6.8. Prohibited Uses

6.8.1. Any use that is determined to be inconsistent with this policy or other policies, rules or regulations of the Corporation is prohibited. The following activities, in addition to those outlined in the policy, are prohibited at all times on any IT resources:

6.8.1.1. Intentionally sending files or messages containing programs designed to disrupt other systems (commonly known as viruses);

6.8.1.2. Accessing another computer system without authorization inside or outside of the Town's network (commonly known as hacking);

6.8.1.3. Intentionally possessing, using, or transmitting unauthorized material, in violation of copyright restrictions;

6.8.1.4. Storing files that are not work related on the corporate network;

6.8.1.5. Installation of software in violation of software licensing and piracy restrictions;

6.8.1.6. Creating, viewing, storing, printing or re-distributing unlawful or potentially offensive material or information on any computer system accessed through the Town's network (this includes sexually explicit, obscene, or other potentially offensive material);

6.8.1.7. Users must take extra care while accessing/opening Electronic Messages or attachments from unknown senders on either Town email or personal email accounts. Users must not follow the link(s) on spam messages; and,

6.8.1.8. Using the Town's equipment services for private financial gain, commercial advertising or solicitation purposes.

6.8.2. Users must refrain from:

6.8.2.1. Changing the configuration or attempting to circumvent or subvert security measures on operating systems and software, unless this activity is a part of your normal job/duty;

6.8.2.2. Using IT Resources and other resources in such a way so as to incur lawsuits or other liability against the Town (e.g., by violating copyright laws, creating and distributing false financial data, making defamatory allegations, etc.);

6.8.2.3. Engaging in any activity that might be purposefully harmful to the IT Resources, systems or to any data stored thereon, such as propagating malicious programs, installing unauthorized software, making unauthorized modification to data or using any program or command in a manner that can degrade the system performance and/or deny services to authorized Users; and,

6.8.2.4. Making copies of any the Town's software, applications or utilities for use outside the Town.

6.9. Reporting Misuse

6.9.1. Users should promptly report any allegations of misuse to their Supervisor as well as the Manager of Information Technology.

6.9.2. Users who receive an offensive email shall refrain from forwarding, deleting, or responding to the message and instead report it directly to Information Technology Services.

6.10. Enforcement

6.10.1. Failure to comply with this policy may result in disciplinary action, up to an including termination of employment.

6.10.2. Violations of the policy that are also violations of the law shall result in referral to law enforcement authorities.

6.10.3. Employees and members of council who violate this policy may also be required to compensate the Town for any damages or costs whether direct or as a consequence of the failure to adhere to his policy.

7. RESPONSIBILITIES

7.1. **Council** has the authority and responsibility to:

7.1.1. Adopt the Information Technology Acceptable Use policy.

7.2. The **CAO** has the authority and responsibility to:

7.2.1. Ensure appropriate oversight is in place within respective areas of responsibility to ensure compliance with the policy.

7.3. All **Directors, Managers and Supervisors** have the authority and responsibility to:

7.3.1. Ensure policy is followed and where clarification is required, provide to ensure policy compliance.

7.4. The **Manager of Information Technology Services** Division has authority and responsibility to:

7.4.1. Grant permission to share accounts, log-ins and passwords.

7.4.2. Approve the alteration of security settings, virus protection or the bypass of firewall protections.

7.4.3. Approve all software and applications used by the Town.

7.5. **Staff** have the responsibility to:

7.5.1. Ensure their understanding and compliance with the policy and seek clarification where needed to follow the policy expectations.

7.5.2. Report any known or suspected violations of this policy immediately to their Supervisor and Manager of Information Technology.

8. LEGISLATIVE REFERENCES

8.1. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

8.2. Employment Standards Act, 2000