TOWN OF AMHERSTBURG

POLICY NO.: TECHNOLOGY USE POLICY

SOURCE:	**Information Technology Department**
SECTION:	
DATE ENACTED:	**March 22, 2010**
DATE OF AMENDMENT:	**Feb 6, 2012**

1.0 POLICY OVERVIEW

1.1 Policy Statement

The Corporation's information technology environment greatly increases our ability to adapt technology to business needs across the Corporation. Technology allows employees and members of council to communicate with others, obtain and share information.

This policy identifies roles, responsibilities, and requirements for appropriate use of corporate technology. Authorized users are granted permission to use data, systems, technologies, and devices that belong to the Corporation in accordance with this policy.

1.2 Purpose

This policy is intended to protect the Corporation and its information technology infrastructure against hazards such as:

- unauthorized access
- malicious manipulation and/or destruction of information/data
- virus invasion
- inappropriate use
- litigation due to misappropriation of software and/or data
- inappropriate disclosure of personal information

Compliance with the policy will also ensure data integrity and security and prevent employees and members of council from using technology to misrepresent the Corporation.

Email is a critical mechanism for business communications at the Corporation. However, use of the Corporation's electronic mail system, services, and devices is a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the Corporation. One of the objectives of this policy is to outline appropriate and inappropriate use of the Corporations e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

The Internet enables employees and members of council to gather information relevant to the Corporation and its businesses from external sources. The Internet also enables the research of relevant topics and to obtain and prepare useful business information. One of the objectives of this policy is to outline the appropriate and inappropriate use of the Corporations Internet resources, including the World Wide Web, electronic mail, the intranet, and FTP (file transfer protocol).

Communication hardware, such as telephones, two-way radios, electronic organizers/PDA's (i.e. Blackberry), pagers, cell phones, fax etc... allow employees and members of council of the Corporation to communicate with other employees and members of council, vendors and business contacts. This policy will also outline the appropriate and inappropriate use of the Corporation's communication hardware.

2.0 POLICY

The goal of this policy is to protect the Corporation from legal liability and to reduce the risk of damage, loss, or theft to corporate technology resources and devices.

2.1 Scope

This policy applies to anyone who directly or remotely, including from home or via Virtual Private Network, has access to the Corporation's information technology infrastructure, applications, files, e-mail, any other technical services or communication hardware.

2.2 Account Activation/Termination

The level of access employees and members of council have to the Corporations computers, networks, applications, internet services, email services and communication hardware is based upon specific job requirements. Employees and members of council must have approval of a department head and Corporate and Legislative Services in order to gain access to the above technology. Without the approval of the department head and Corporate and Legislative Services, access shall not be granted. Each user is 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. It is the responsibility of the employee or member of council to protect the confidentiality of their account and password information. Access will be terminated and any communication hardware will be returned when the employee or member of council terminates their employment with the Corporation, unless other approved arrangements are made. The Corporation is under no obligation to store or forward the contents of an individual's email inbox/outbox, data stored on the network, or data stored on communication hardware after the term of their employment has ceased.

Each employee's or council member's password must be confidential and strong. The employee or member of council should not share his/her password with anyone or leave it where someone else could access it. The network system requires employees and members of council to change their passwords on a regular basis. In order for your password to be considered strong, passwords should be alphanumeric, and should not be proper names, places or personal information. If an employee or member of council has concerns about how to create a strong password, they should contact the Information Technology group for assistance.

2.3 Acceptable Use

Employee and council member access to the Corporation's computers, networks, applications, internet services, email services and communication hardware are to aid employees and members of council in the performance of their employment responsibilities.

2.4 E-Mail

The Corporation's information technology systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on the Corporation's information technology systems. Email use at the Corporation will comply with all applicable laws, all Corporations' policies.

E-mail is a critical mechanism for business communications at the Corporation. E-mail has been provided to assist and enhance communication. All e-mail accounts must be approved by the appropriate department head and Corporate and Legislative Services. All accounts must be accessed using an e-mail program approved by the Manager of Information Technology.

Important official communications are often delivered via email. As a result, employees and members of council of the Corporation with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important corporate announcements and updates, as well as for fulfilling business and role oriented tasks. E-mail users are responsible for mailbox management including organization and cleaning.

Employees and members of council and members of council are cautioned that e-mail is considered a public record under the Municipal Freedom of Information and Protection of Privacy Act. Employees and members of council should assume that any e-mail may be deemed "public information" and treated the same as any other written communication. The decision to send personal information through e-mail should be considered when making this information available to other employees and members of council. In no circumstances should e-mail containing personal information be forwarded or copied to individuals outside the Corporation unless the individual to whom the information relates, consents to the disclosure and is copied on the e-mail.

Employees and members of council are cautioned to avoid using e-mail and other 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.

Employees and members of council shall not make the name and e-mail addresses of other employees and members of council available to those whose intent is to communicate with employees and members of council for purposes unrelated to their job responsibilities.

Sending of unreasonable large e-mail attachments should be avoided unless authorized by department head. The total size of an individual e-mail message sent (including attachments) should be 5MB or less. Assistance from Information Technology Services will be required should there be a need to either send or receive e-mail messages larger than 5 MB.

Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, slander, fraud, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (example: spreading of computer viruses) is strictly prohibited.

2.5 File/Data Storage

It is the responsibility of each employee and member of council o regularly delete messages/files that are no longer required. Due to storage capacity limits on the corporate network, each employee and member of council is allocated a certain amount of storage space. If the limit is exceeded, you will be notified via a System Administrator message to delete some of the stored e-mail and/or working files. Files that are not work related are not to be stored on the corporate network including but not limited to computers, network storage, portable storage devices and pda's

2.6 Internet and Websites

Internet access is provided primarily for research in connection with an employee's or member of council specific job duties. Employees and members of council are reminded that use of the internet must not interfere with an employee's or member of council job duties. The growing use of the internet is a perfectly acceptable means of obtaining work related information. However, it is unacceptable to "surf the net" for personal purposes on work time.
Only software approved by the Manager of Information Technology may be used to browse the internet. 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.

2.7 Privacy

The Corporation retains control, custody and supervision of all computers, networks, internet services, e-mail services and communication hardware usage. The Corporation reserves the right, at any time, to inspect and/or monitor system files, logs and other activity including e-mails stored on any server or individual computer. Monitoring may also include surveillance programs designed for that purpose, see Section 5.

2.7.1 Town Property

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.

2.8 Security

The Corporation employs various measures to protect its equipment and data from deliberate or inadvertent destruction or misuse. Such measures include the designation of individual accounts, log-ins, and passwords. Sharing of accounts, log-ins and passwords is prohibited unless approved by the Manager of Information Technology grants an exception.

The Corporation also uses a variety of other means to protect its systems and data including security settings in software applications, virus scanning software and firewalls. 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.

Computers, PDA's or data storage devices that are not directly managed by the Information Technology dept are not to be connected to the Corporations networks whether directly or via virtual private network or other remote access technologies.

2.8.1 Personal Computer and Device Security

All computers and smart phone devices shall be configured to have a password-enabled screen saver. This security lockout feature shall automatically initiate after the computer or smart phone remains idle from user interaction after a 15 minute time period. The user must then re enter their password to gain access to the computer or smart phone. The general best practice for enabling automatic lockout of a screen saver is to set the timeout so that it can provide adequate security and not be inconvenient to the user. This applies to all internet access inclusive of PDA devices and smart phones including but not limited to Blackberry devices

2.9 Personal Use

Personal use of the Corporation's computers, networks, internet services, e-mail services, telephone and other communication hardware should be minimal and must not interfere with the performance of the employee's or member of council job duties and be consistent with appropriate professional conduct.

Employees and members of council are reminded that all personal use must comply with this policy as well as all other procedures, regulations and laws. Employees and members of council are further reminded that all use may be monitored and inspected.

Employees and members of council shall not install, or attempt to install, on any Corporation's computer systems, personally owned software, shareware or freeware, unless approved by their respective department head and the Manager of Information Technology. If any non-approved software is found to be installed on any computer or server, it may be removed without notice. Any use of the Corporation's equipment or services for private financial gain, commercial advertising or solicitation purposes is prohibited.

2.9.1 Personal Email Accounts

Use of personal email accounts is prohibited. Examples include but are not limited to hotmail, Gmail, Yahoo Mail, AOL. This applies to all internet access inclusive of PDA devices and smart phones including but not limited to Blackberry devices

2.9.2 Internet Relay Chat

Use of internet relay chat sites and software is prohibited. Examples include but are not limited to Windows Live Messenger, Yahoo

Messenger, and Paltalk Messenger. . This applies to all internet access inclusive of PDA devices and smart phones including but not limited to Blackberry devices

2.9.3 Social Networking Sites

Use of social networking sites is prohibited. Examples include but are not limited to face book, my space, twitter, classmates.com.. This applies to all internet access inclusive of PDA devices and smart phones including but not limited to Blackberry devices

2.10 Copyrights

It is the policy of the Corporation to fully comply with all laws pertaining to the reproduction, use or distribution of copyrighted or otherwise protected materials. The Corporation will comply with all licensing requirements. Employees and members of council shall not make copies of software other than those copies authorized in the software license. Employees and members of council shall respect the copyrighted protection of materials found on the Internet.

2.11 Prohibited Uses

Any use that is determined to be inconsistent with this policy or other policies, rules or regulations of the Corporation is prohibited. In addition to the prohibited uses cited throughout this policy, other prohibited uses include but are not limited to:

- Any use that is illegal.
- Any use involving materials that are pornographic, violent, obscene, hate propaganda, sexually explicit or sexually suggestive.
- Any use that represents personal views as the views of the Corporation.
- Malicious use or deliberate disruption of the Corporation's computers, networks, internet services, e-mail services or communication hardware and/or breach of security features.
- Misuse or deliberate damage to the Corporation's computer systems and/or components.
- Copying, downloading, installing/removing software or applications without the approval of the Manger of Information Technology.
- Using network system resources for the storage of non-business related data or information (e.g. personal photos, games, music).Use of corporate technology systems, services and devices for unsolicited mass mailing, non Corporation commercial activity, dissemination of chain letters, and use by non-employees and members of council.

2.12 Reporting Misuse

Any allegations of misuse should be promptly reported to your supervisor as well as the Manager of Information Technology. If you receive an offensive e-mail, do not forward, delete or reply to the message. Instead, report it directly to Information Technology Services.

2.13 Amendments

The Corporation may amend and supplement this policy from time to time. Employees and members of council will be provided with any amendments and supplements and are expected to abide by them.

3.0 ENFORCEMENT

It will be the responsibility of the employee's department head, in consultation with the Manager of Information Technology, to determine the appropriate response to infractions. All disciplinary action will be in accordance with the Corporation's discipline process.

4.0 CONSEQUENCES

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Violations of the policy that are also violations of law may result in referral to law enforcement authorities. Employees and members of council who violate this policy may also be required to compensate the Corporation for any damages or costs whether direct or as a consequence of the failure to adhere to this policy. The Corporation will not make job accommodations to individuals who have, by virtue of inappropriate conduct, lost the privilege of using the Corporation's computers, systems, internet services, e-mail services or communication hardware.

5.0 MONITORING

Utilities are in place to monitor Internet usage, e-mail, file storage and corporate computer configurations.

The Corporation, through the Corporate and Legislative Services Department, may monitor an individual's information or electronic data to ensure appropriate use. Monitoring will also assist in protecting the security of the corporate computing environment.

By way of this policy, Corporate and Legislative Services is also fully authorized to review former or current employee or member of council information (i.e. e-mail, files, Internet access) without notice at any time as required to meet legal obligations.

It is understood that Senior Management Team deals with highly confidential issues on a regular basis. In the event that the monitoring tools identify a potential threat to our environment, and the e-mail and/or document in question is to/from a member of the Senior Management Team, then the information will only be accessed by the Manager of Information Technology or Chief Administrative Officer for the purposes of security.

5.1 Regular Random Auditing

Regular random auditing will be performed across the organization without any prior notice at any time. Auditing is inclusive of all devices and means of communication, including but not limited to smartphones, mobile tablets, cell phones, email, computers and laptops.

6.0 DEFINITIONS

Alphanumeric – containing both numbers and letters.

Corporate Technology– includes computer/network hardware, software and/or communication hardware (computers, cell phones, regular telephones, PDAs (personal digital assistants), pagers etc.), used to support the business of the Corporation.

Firewall - 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.

FTP (file transfer protocol) - the simplest way to exchange files between computers on the Internet; commonly used to download programs and other files to your computer from other servers.

Intranet – the network contained within the Corporation. The main purpose of an intranet is to share company information and computing resources among employees and members of council.

Media – tools used to store information, especially computer hard drives, floppy drives, compact discs (CDs) and digital versatile discs (DVDs) used to store files.

PDA – (personal digital assistants) - handheld devices used to store information such as: e-mail, appointments, calendar, files. This includes Blackberries, Smartphones, and other computer-like devices.

Personal Information - refers to recorded information about an identifiable individual and includes information recorded via electronic means. Personal information should not be collected, used or disclosed except in accordance with the Municipal Freedom of Information and Protection of Privacy Act.

Senior Management Team – the Senior Management team is made up of all of the department heads within the Corporation.

Streaming Media Application - multimedia that is constantly received by, and normally displayed to, the end-user while it is being delivered by the provider. This includes listening to the radio and/or watching movies via the Internet.

Virtual Private Network - a network that uses a public telecommunication infrastructure to connect remote offices or individual users with secure access to the Corporation's network.

Virus – a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD. Virus Invasions/Infections can potentially prevent the corporation from doing any business by preventing critical systems from running properly.

World Wide Web - all the resources and users on the Internet that are using the Hypertext Transfer Protocol (http://); also can be defined as the universe of network-accessible information, an embodiment of human knowledge.

7.0 REFERENCES

Employee Code of Conduct Policy