Corporate Policy Manual

Sub Topic: Internet & e-Mail Acceptable Use	Policy No. IT.1-01
Topic:	Employees Covered: All Employees All Elected Officials
Section: Information Technology	Council Adoption Date: October 11, 2005
Effective Date: October 11, 2005	Revision No: Date:

Policy Statement

Town employees are responsible individuals and put forth an honest effort in the performance of their duties. This policy is intended to help employees and elected officials who use Town computer systems, draw the line between acceptable use of computers and their abuse. Today's information technology magnifies any error in judgment in its use. The Town must therefore take reasonable measures to ensure that its employees and elected officials who use Town computers understand the difference between legitimate and inappropriate uses.

The relationship between the Town and its employees and elected officials is founded on trust. This policy reflects a balance between the obligation of the Town and its employees and elected officials. The Town must ensure that its computers are used appropriately. Employees and elected officials are provided with a professional and supportive work environment. They are given access to the tools needed to effectively and efficiently carry out the assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps the Town retain highly qualified and skilled employees.

Purpose

Access to internet activities enables employees and elected officials to research information relevant to the Corporation's business from external sources, and to provide information to residents, potential residents, businesses and business prospects. Employees and elected officials have access to these systems consistent with the requirements of their job, and are encouraged to use these systems. The Corporation's goal is to ensure that the e-mail and internet systems continue to be a reliable and productive tool for the Corporation.

Definitions

"***C:drive***" is the part of a unit, often called a "hard disk", "disk drive", "hard drive" or "hard disk drive", that stores and provides relatively quick access to large amounts of data on an electromagnetically charged surface or set of surfaces. In a networked environment, such as the Town's, the C:drive is the storage location for files that are not part of the network. The C:drive is not backed up nor serviced by IT, unless specifically requested to do so.

"***Downloading***" is transmission in the other direction – from one, usually larger computer to another, usually smaller computer. From an Internet user's point-of-view, downloading is receiving a file from another computer.

"***e-mail***" means a system for sending and receiving messages electronically over a computer network, as between personal computers.

"***employees***" includes all regular full time, part time, contract employees, contractors, casual, sessional/seasonal and consultants retained by the Town.

"***Executable/Non-Executable Files***" means in computers to execute a program is to run the program in the computer. An executable is a file that contains a program – that is, a particular kind of file that is capable of being executed or run as a program in the computer. A file whose name ends in ".exe" is really a program that when "opened" – that is, selected by putting your mouse over the file name and then initiated by double-clicking your mouse, for example – causes that operating system to run the program. Users who receive an .exe file as an e-mail attachment should always be sure that the file comes from a trusted source and is not, in fact, a computer virus. Executable files are a common vehicle for transmitting a virus.

"***Hoax***" means a false warning about a computer virus.

"***Internet***" means the international computer network known by that name.

"***Internet Activities***" means all activities undertaken through the Corporation's internet resources including electronic mail and browsing external web sites unless otherwise specified.

"***PDF (Adobe)***" means Portable Document Format. This is a file format that has captured all the elements of a printed document as an electronic image that you can view, navigate, print or forward to someone else, however, that cannot be modified. PDF files are created using Adobe Acrobat, or similar products produced by the company Adobe.

"***Push or Pull Technology***" is the pre-arranged updating of news, weather or other selected information on a computer user's desktop interface through periodic and generally unobtrusive transmission over the World Wide Web (including the use of the Web protocol on intranet). Push (or "server-push") is the delivery of information on the Web that is initiated by the information server rather than by the information user, as it usually is. Pull is the term used for information that is provided as a result of a request for that information.

"***Software***" is a general term for the various kinds of programs used to operate computers and related devices.

"***Uploading***" is the transmission of a file from one, usually smaller computer system to another, usually larger computer system. From a network use's point-of-view, to upload a file is to send it to another computer that is set up to receive it.

"***Virus***" means, in computers, 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. The immediate source of the e-mail note, downloaded file, or diskette you've received is usually unaware that it contains a virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and effect ("Happy Birthday, Ludwig!") and some can be quite harmful, erasing data or causing your hard disk to require formatting. A virus that replicates itself by re-sending itself as an e-mail attachment or as part of a network message, is known as a worm.

Generally, there are three main classes of viruses:

> **File infectors**. Some file infector viruses attach themselves to program files, usually selected .COM or .EXE files. Some can infect any program for which execution is requested, including .SYS, .OVL, .PRG and .MNU files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly-contained programs or scripts sent as an attachment to an e-mail note.
>
> **System or boot-record infectors**. These viruses infect executable code found in certain system areas on a disk. A typical scenario is to receive a diskette or file from an innocent source that contains a boot disk virus. When your operating system is running, files on the diskette can be read without triggering the boot disk virus. However, if you leave the diskette in the drive, and then turn the computer off or reload the operating system, the computer will look first in your A drive, find the diskette with its boot disk virus, load it, and make it temporarily impossible to use your hard disk.
>
> **Macro viruses**. These are among the most common viruses, and they tend to do the least damage. Macro viruses infect your Microsoft Word application and typically insert unwanted words or phrases.

Procedures

Ownership

Town computers that provide internet/intranet and e-mail privileges are considered Corporate assets and are intended to be used for business purposes only.

All data created and stored on Town computers remains the property of the Corporation of the Town of Newmarket. Employees and elected officials are therefore cautioned

against storing any personal information on Town computers. All information stored on the Town network becomes a corporate record and there is no guarantee that personal information will remain private. Because Town computers are often reconfigured or redeployed inside and outside the organization, there is always the potential that personal information could be exposed at some point in time. The use of the Town's computers for personal information is NOT RECOMMENDED.

E-mail and Internet Access

E-mail access via internet is automatically provided to all employees and elected officials who require access for the purposes of their job. Additional approval is not required.

Access to other internet activities is determined by the requirements of the employee and the elected official's position. It is the responsibility of the Director of each department to assess employee needs when granting access. Functions available will vary from time to time depending upon technological developments and Corporate Policy. Requests for internet access must be submitted to the Manager of Information Technology or designate. All employees must receive the prior approval of their Director or Commissioner.

Privacy of communications – e-mail and Internet

Correspondence via internet e-mail is NOT guaranteed to be private. It is susceptible to interception by non-legitimate means. While network administration provides a high level of privacy and security on the network, users should be aware that e-mail messages and other files can be recovered even though deleted by the user. The Information Technology Division will only recover deleted e-mails when requested by the employee or elected official to whom the e-mail relates, or when directed to recover deleted emails for legal purposes.

E-mail and Internet Data security

Employees and elected officials must safeguard their login ID and password from disclosure to any person. Users must use their own login ID and password, are responsible for all activity on their log in ID, and must immediately report any known or suspected compromise of their ID to the Information Technology Division.

E-mail and Internet Monitoring

The Town monitors all computer systems usage to ensure proper working order, appropriate use by employees and elected officials, and the security of corporate data. The Manager of Information Technology, Commissioners/Departmental Directors of each Business Unit and the CAO or their designates may access user files relating to the department(s) for which they are responsible. Such access to user files includes the ability to retrieve archived materials of present or former employees and elected officials without the user's consent for purposes relating to maintaining the integrity of the network, or exercising the rights of the Corporation or other users for any reasonable purpose.

Sending E-Mail Messages to “All Employees”

E-mail messages sent to all employees also go to the Library, Fire Hall, all Members of Council and all outside facilities. In addition, some messages are forwarded to personal e-mail addresses at homes such as those of elected officials. Employees and elected officials are therefore asked to refrain from e-mailing messages to all employees without first consulting their Manager, Director/Commissioner or CAO.

The Town’s intranet service will eventually reduce the need to send messages to all employees and elected officials. Employees and elected officials will receive instruction on the use of the intranet once it is in service.

Personal use of internet and e-mail

Personal use of the Town’s computer systems is only authorized in accordance with the Guidelines as amended from time to time.

Downloading

Downloading of non-executable files for business use is permitted. These include reports, Adobe PDF files, information flyers, etc., from other institutions or government agencies that may be useful to the Corporation.

Executable software, including files containing embedded executable codes, may not be downloaded. This type of software may contain viruses that could harm the Corporation's network. If such a file is required, it must be downloaded by the Information Technology Division who will then check the file for any infection.

The sending and receiving of large attachments is discouraged, as attachments are susceptible to viruses. Employees must use extreme caution when opening e-mail attachments, which may contain viruses.

Unsolicited E-mail and Computer Viruses

Individuals in the organization may receive unsolicited e-mails. Some e-mails are fraudulent solicitations and some e-mail is offensive. An individual who receives unsolicited or offensive e-mails is a victim, and such individual should report any unsolicited e-mails to the Manager of Information Technology. In order to prevent viruses and other intrusions to the Corporation’s e-mail services, employees should never open any suspicious e-mail message. Any suspicious e-mail messages should be reported to IT Staff immediately. While the Town has recently installed software on each desktop to check for viruses or other problems that could cause a computer to malfunction, employees should always exercise caution.

Freedom of Information

All electronic documents which are created by or with the Corporation's computers or network, including internet related systems, are records for the purposes of the Municipal Freedom of Information and Protection of Privacy Act, the Freedom of Information and Protection of Privacy Act, and other related legislation and regulations and may be a public record for the purposes of the legislation.

Amendments

The Corporation may amend this Acceptable Use Policy from time to time as necessary. All employees and elected officials with access to Internet-related systems will receive prompt notice of any amendments.

Disclaimer

The Corporation will not be responsible for any misuse of corporate internet related systems. In addition to any other discipline measures, persons found to be intentionally misusing the Corporation's internet-related systems will be responsible for any costs or damages sustained by the Corporation or a third party and will be obligated to indemnify the Corporation for any claim against the Corporation by a third party.

Cross Reference

Employee Code of Conduct (currently under development)
Council Code of Conduct (currently under development)
Progressive Discipline Policy HR.4-01
Harassment & Discrimination Free Workplace Policy HR.5-01
Administration By-Law