City of Carlton

SUBJECT: **Use of Information Technology**

Policy

City computers, Internet access and E-mail are tools that will help us be more efficient in our jobs. They are to be used to conduct City business. E-mail messages received or sent on City computers are City records and property. The City has the right to monitor employee use of the Internet and e-mail as well as the right to monitor City computers and audit their contents. Use of the internet and e-mail is a privilege that may be revoked if it is abused. It is the objective of this policy to increase productivity and decrease risks to network security and performance, protect the privacy, integrity and security of City information, increase adherence to City information and technology-related policies and standards, and to promote public trust in the City's use of information and technology assets. Each employee who violates this policy may be subject to disciplinary action up to and including termination from employment.

Purpose

All users of the City's information and technology resources must take responsibility for, and accept the duty to, actively protect information and technology assets. This includes taking responsibility to be aware of, and adhere to, all relevant policies and standards. The City's uses of information technologies to support employees and other authorized users to work efficiently in delivering services to residents. Proper use of these technologies assists in the daily management of information, saves time and money, reduces administrative overhead and improves service delivery. The technologies include, but are not limited to, information systems, services (e.g. web and messaging services), computers (e.g. hardware and software), and telecommunications networks and associated assets (e.g. telephones, facsimiles, cell phones, laptops, personal digital assistants). Improper use may jeopardize the confidentiality, integrity and availability of the City's information and technology assets, and may put personal information protection, security or service levels at risk.

Liability

Material obtained from the Internet may be protected by copyright laws. Therefore, each employee is obliged to determine whether copyrighted information can be used for official purposes. Generally, material from governments and public institutions is part of the public domain and not subject to copyright protection. Profanity and obscenity should not be used on the internet and e-mail. Personal use of the internet and e-mail should follow the same restrictions that apply to use of the telephone as detailed in the city Personnel Policy.

Downloading of Files

Computer viruses, "adware", "spyware", "malware" and "trojans" may be present in files that are downloaded or copied from the Internet to a City PC. To help protect the City Network from these malicious programs, our firewall and spam filter contain software that will identify and clean most of these harmful viruses and programs but no system is completely secure.

Use of Information Technology

1. **Users must** use City provided information technology resources as business tools required to do their work and provide efficient service delivery. This use is subject to the same restrictions and management review process as any other City resource.

2. **Users mu**st take precautions to prevent security breaches and/or damage to technology equipment. This includes protecting the confidentiality of sensitive customer information, protecting user passwords and PIN numbers as well as protection against computer viruses, spyware and malicious code from outside sources.

3. **Users shall not:**
a. attempt to circumvent or subvert system or network security measures.
b. propagate viruses knowingly or maliciously.
c. detrimentally affect the productivity, integrity or security of City systems.
d. attempt to add, modify and/or upgrade any hardware, software and firmware to City systems without the direct consent and involvement of a member of the City's IT department. IT personnel strongly discourage employees from using personal technology equipment attached to the City's network or at any City facility. If the need should arise and there is justification for the use of personal equipment, the user must have the permission of the City's IT department and understand that the City will not be responsible for the maintenance, repair or replacement of the equipment.
e. obtain files from unauthorized or questionable sources (e.g., racist, material, pornography, file swapping sites).
f. access Internet sites that might bring the public service into disrepute or harm the City's reputation, such as those that carry offensive material.
g. download non-work related files, such as Freeware, Shareware, movie or music files.
h. divulge, share or compromise their own or another's authentication credentials.
i. transmit or otherwise expose sensitive or personal information to the internet.
j. use information and technology resources for commercial solicitation or for conducting or pursuing their own business interests or those of another organization.
k. distribute hoaxes, chain letters, or advertisements.
l. send rude, obscene, or harassing messages.
m. send, forward and/or reply to large distribution lists concerning non-City related business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists.
n. attempt to obscure the origin of any message or download material under an assumed internet address.

4. **Users shall:**
a. comply with all applicable legislation, regulations, policies and standards.
b. use all appropriate anti-virus precautions when accessing non-City data and systems from the City network.
c. adhere to licensing agreements for all software used.
d. access radio stations or video clips (typically referred to as "streaming" audio or video) over the Internet as long as the extent of such usage does not adversely affect the bandwidth available for work purposes.
e. respect copyright and other intellectual property rights in relation to both programs and data
f. use approved security measures when accessing the City's network from home or from a non-City computer.

g. only use messaging forums (e.g., internet Relay Chat, internet newsgroups) when conducting work-related business exchanging technical or analytical information.

h. use hard passwords for system and network access.

5. Any content created or transmitted using City equipment or retained within the
City network will be managed as a public record. There is no expectation of personal privacy related to the use of City information technology resources except for specific privileged communications (i.e. Human Resources).

Approved: ______________________________

Mayor: _________________________________