Information Technology General Use and Practices

Procedure number:	A-ISS-001-001
Parent policy number:	A-ISS-001
Section:	Administration
Sub-section:	Information systems
Author(s):	Information Systems
Authority:	CAO
Effective date:	2006-07-04
Review by date:	*5 years from CAO approval*
Last modified:	*CAO approval date*

Purpose statement

This procedure defines the standards and guidelines for the acceptable use of information technology resources. The areas covered include, access and security, internet and electronic mail (email) use, the use of software, hardware and all related devices, and examples of unacceptable uses of ~~personal accounts~~town information technology resources.

Scope

This procedure applies to all users including town employees (including but not limited to full-time, part-time, students, volunteers, temporary and interns), elected officials, and any individual representing or acting on behalf of the town in any manner, with authorized access to and who use town provided information technology (IT) resources.

IT resources for the purpose of this procedure include, but are not limited to; voicemail, telephones, internet, intranet and email system(s); electronic data transmission equipment and devices, software and hardware, portable media, storage devices, network(s), point of sale equipment, radios and other audio-voice communication equipment and video systems.

Procedure

1. Access and Security

The confidentiality and integrity of data stored will be protected by access controls to ensure that only authorized users have access. This access will be restricted to only those capabilities that are appropriate to each user's job duties.

~~Directors~~ Leadership must notify the ~~IS~~ Information Technology and Services department (I.T.S.) immediately, of terminations, retirements, resignations, extended absences, transfers or re-assignments of employees, so that access privileges can be modified or revoked.

To ensure high standards of security and protect corporate information, users must adhere to the User Security Settings and System Configuration procedure.

2. Compliance with Applicable laws, Regulations and Corporate Policies

Information technology resources must be used in compliance with applicable laws or regulations, professional standards, software licensing agreements and Corporate Policies and procedures including but not limited to Respectful Conduct Policy and Codes of Conduct.

3. Freedom of Information and Protection of Privacy

Information technology resources are to be used in a manner consistent with the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and applicable ~~Corporate~~ corporate ~~Policies~~ policies and ~~Procedures~~procedures. Voicemail, pictures, videos, ~~and~~ email messages, as well as text and other instant messages , created on any town issued information technology resource (which includes both software and hardware) are considered to be a matter of town~~corporate~~ record under the provisions of *MFIPPA* ~~and must be saved and stored for reference~~. I.T.S. maintains secured copies of all emails to fulfill these legislated email retention requirements, but ~~staff~~ users should maintain copies of pertinent voicemail messages, pictures, ~~and~~ video files, as well as text and other instant messages, and have them securely stored with their other electronic files. I.T.S. has the ability to convert voicemail messages to an electronic file, such as mp3, to facilitate ease in storage. Users, uncertain which messages to save, should consult with their supervisor.

4. Ownership

Anything stored or resident on the town systems and all information technology resources acquired and managed by the I.T.S. department remain property of the town. Additionally,

all equipment provided by the town remains the property of the Town of Oakville, and at the end of its useful life, must be returned to the I.T.S. department for proper disposal.

5. Personal Use

Occasional or incidental personal use of information technology resources is permitted within reasonable limits, provided it does not conflict with business use or time, or impact negatively on other users or on the information technology resources, or adversely affect an individual's performance of work duties and responsibilities. Users are responsible for exercising good judgment regarding the reasonableness of personal use. The systems and resources furnished by the town remain the property of the town. Therefore, all users are responsible for their actions while using any town resource or network. The town reserves the right to view, change or modify files located anywhere on the network for the purpose of support, best practices, improvements or when issues arise. Any person in violation of Human Rights laws, or Corporate Policies and procedures is subject to disciplinary action.

~~Personal time is defined as a maximum 60-minute period in increments of 10-minutes that users can search and use the Internet for personal reasons in recognition that computers may be used at lunch and breaks. This personal time is a privilege and should be used ethically and responsibly. I.T.S. may need to modify the use of personal time based on technical constraints and changes in organizational decisions. At no time will Personal Use extend to the usage of Town of Oakville equipment for personal gain or profit or for personal business use.~~

6. Monitoring

The town respects the privacy of users, however the town reserves the right to monitor all town information technology to ensure proper working order, appropriate use by employees and security of the corporate data without user consent. The town may delete, intercept or block any traffic on its networks, to prevent spam, pornography, hate related material, or illegal use of town property and violation of town policy and procedure.

7. Preserving Assets

Town information technology resources are valuable assets and users of such are expected to exercise reasonable care to prevent abuse to, theft of, or excessive wear of town information technology resources.

Users will exercise care with town property and will secure equipment when travelling or transporting equipment. Laptops and accessories should not be left in a vehicle. Devices are required to use password protection to secure confidential information.

Where and whenever equipment has been lost or stolen, the loss shall be reported immediately to the employees' manager as well as I.T.S. This reporting will ensure communication tools or devices can be removed from networks and will mitigate risks that may arise, where issues with compliance may occur or where breaches of confidential information may be impacted.

8. Internet Access

Access to internet is provided to users to facilitate town business. It is a breach of the Use of Information Technology Resources Procedure to access websites that contain any form of material of a nature that is pornographic, obscene, hateful, offensive; or other objectionable materials.

Information may be downloaded from the internet for town business purposes; such information includes reports, spreadsheets, presentations, information files, etc. from other institutions and government agencies that may be useful to the town. The use of audio or video streams from the town's intranet or internet sites is permitted for business use only. Use of audio or video streams and the use of audio/video communication tools for topics not related to the interest of the town are prohibited and should be limited to business use with prior consent from the I.T.S. department. Examples of audio/video communication tools may include media video sites such as YouTube, iTunes radio and satellite radio streaming, Skype, iChat, VOIP Buster etc.

Executable software (programs) may not be downloaded, and will not be available for installation. If software is required, a request to the I.T.S. department via the Help Desk, should be made in order to ensure licenses are available.

The I.T.S. department will monitor internet use and block access to some web sites that pose system risks and are not in compliance with the Information Technology General Use and Practices -Policy and Procedure.

9. Email

The town's email service is provided to communicate messages and attach electronic files for electronic distribution via the internet and intranet for town business purposes.

Users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the internet are not secure and may be intercepted and disclosed to third parties.

Generally, information which is sensitive or confidential in nature (such as personal information about individuals, employee performance or other human resource issues, information regarding issues to be discussed in closed door sessions, etc.) should not be sent via email, but where required, should be marked confidential.

In addition, similar to the Personal Use section, employees recognize the town's systems belong to the town and should always exercise good judgment in the workplace. If an employee is in violation of the *Human Rights Code* or the Corporate Policies and/or procedures they may be subject to disciplinary action.

10. Use of "Instant Messaging Tools" for Official Town Business: Strongly Discouraged

In accordance with guidance from the Information and Privacy Commissioner of Ontario, the town's Record Retention By-law and applicable corporate policies and procedures, the town-provided instant message tools, including text messaging (SMS), are to be used for transitory and routine communications only to assist in conducting town business. Such communications are subject to *MFIPPA*.

Communications that document and support decisions, activities, and transactions related to town business must be recorded, such as emails, and retained in the town's official recordkeeping repository in accordance with the Records Retention By-law.

11. Use of information technology resources not managed by the town for Official Town Business: Strongly Discouraged

Users are strongly discouraged from using any IT -resources not owned, supplied, or managed by the town (Appendix A) for the performance of their duties and responsibilities.

Users who elect to use IT resources not owned by or supplied by the town for the performance of the user's duties and responsibilities may, through such use, make the IT resources used for this purpose subject to provincial and federal access to information legislation, contractual restrictions, and related town by-laws and policies, and shall cooperate with the town in fulfilling any resultant obligations that arise from such use.

Users who elect to use IT resources not owned by or supplied by the town for the performance of their duties and responsibilities shall ensure that information, records, and data created, accessed, acquired, managed, or reviewed through such use is moved to and stored on the appropriate corporate system as soon as possible, following which it is deleted from the IT resources not owned by or supplied by the town.

~~10.~~12. Software, Hardware and Data Use

All software, hardware, and data (technology resources) acquired for or developed by town users are the property of the town. All such technology resources must be used in compliance with applicable licences, notices, contracts and agreements. Applications and/or data that is subject to licence agreements, may not be reproduced or shared in any form without permission of the vendor.

Technology resources must be acquired from authorized vendors in accordance with the town Purchasing By-law. Technology resource acquisitions shall be centralized within the

I.T.S. department to ensure that all applications conform to corporate technology standards.

All requests for corporate technology resources must be submitted to the I.T.S. department for review, to determine compatibility with current technology resources, and the standard resource that best accommodates the desired request and approval.

Software installed on user systems will be based on an approved list of applications and requested on the System Access Request form. Non-corporate software will be uninstalled and future user access to install will be restricted. Employees shall not download or attempt to install non-approved applications; examples include (but are not limited to) screensavers, file or photo sharing applications, satellite radio streamers, camera drivers, etc.

Original electronic media will be kept by I.T.S. department, and only the appropriate copies of software and documentation will be given to authorized users.

~~11.~~13. Unacceptable Uses of Town Information Technology Resources

In addition to the examples outlined in other sections, examples of unacceptable use of town IT resources include:

Accessing website content that:

a. Promotes pornography.
b. Presents demeaning or derogatory portrayals of individuals or groups or contain any message that is likely to cause deep or widespread offence.
c. Continuous unauthorized media streaming / external web-radio, and web video stations
d. Using accounts to harass, threaten, embarrass or annoy others or to send material considered obscene, abusive, threatening, libelous or defamatory.

In addition, the following activities represent unacceptable use of website and/or user technologies:

a. Soliciting or conducting business for personal gain or profit using Town owned technology or resources.
b. Sending chain letters or junk mail (spamming).
c. Forwarding inappropriate email, graphic or sound files.
d. Misrepresenting the originator of any communication.

e. Downloading and running any executable software, i.e. files with the extension .exe or .com without previous approval from I.T.S. and/or assistance from a member of the I.T.S. department.
f. Using accounts or technology for illegal purposes including the use of pirated or unlicensed software;
g. Using accounts or technology to circumvent copyrights, trademarks of other intellectual property rights;
h. Installing software and applications that is not supported by and or without the authority of the I.T.S. department.
i. Accessing someone else's personal account, or providing the means to do so without proper delegated authority.
j. Deleting or modifying files belonging to other users without consent.
k. Installing or inserting portable media devices such as USB sticks or drives, iPods, MP3 Players and handheld smart phone technologies without a business purpose or use.

~~**12. Lost or Stolen Equipment**~~

~~Users will exercise care with town property and will secure equipment when travelling or transporting equipment. Laptops and accessories should not be left in a vehicle. Cell phones and BlackberriesDevices are required to use password protection to secure confidential information.~~

~~Where and whenever equipment has been lost or stolen, the loss shall be reported immediately to the employees' manager as well as I.T.S. This reporting will ensure communication tools or devices can be removed from networks and will mitigate risks that may arise, where issues with compliance may occur or where breaches of confidential information may be impacted.~~

~~13.~~14. Consequences of Non-Compliance

Users who fail to comply with the I.T.S. General Use and Practices procedure may lose access privileges. Depending upon the severity of the violation, users may be subject to disciplinary action up to and including dismissal. Illegal violations by any user can and will be reported to the appropriate authorities.

~~**COBIT framework objectives:**~~

- ~~AI 4 – Enable Operation and Use~~
- ~~AI 4.3 – Knowledge Transfer to End Users~~
- ~~DS 5 – Ensure Systems Security~~
- ~~DS 5.5 – Security Testing, Surveillance and Monitoring~~
- ~~DS 5.10 – Network Security~~
- ~~DS 5.11 – Exchange of Sensitive Data~~
- ~~DS 7 – Educate and Train Users~~

References and related documents

A-ISS-001-002 Public WiFi Usage and Disclaimer Procedure
A-ISS-001-003 Equipment and System Access Requests Procedure
A-ISS-001-004 User Security Settings and System Configurations Procedure
Municipal Freedom of Information and Protection of Privacy Act
The Ontario Human Rights Code
Respectful Conduct Policy
Code of Conduct
The Copyright Act
The Criminal Code of Canada
Records Retention By-law
Purchasing By-law of the Town of Oakville
Highway Traffic Act
Use of Town Vehicles, Equipment and Facility Resource(s) Policy

Definitions

Instant message tools: means a type of online chat that offers real-time text transmission over the internet.

Transitory records: means a record that has temporary usefulness and is only required for the completion of a routine action, or until superseded.

Responsibilities

Users are responsible for:

a) adhering to the I.T.S. General Use and Practices Policy and all underlying procedures;
b) all activities on personal accounts;
c) ensuring confidential information is handled appropriately;
d) reporting any known or suspected violations to the immediate supervisor or manager.

Management is responsible for:

a) making employees aware of the -I.T.S General Use and Practices Policy and all underlying procedures, and reporting any contraventions of same;
b) ensuring that access rights of employees are issued or revoked in a timely manner when changes are required;
c) ensuring that any town owned hardware/software is returned to the town.

The I.T.S. department shall in conjunction with other departments, provide leadership, management and control over corporate data application systems and software in order to ensure corporate strategies are supported and that information to manage the town is standardized, consistent and reliable.

The I.T.S. department is responsible for:

a) establishing hardware, software, video and communications technology standards to ensure a secure and reliable information technology and communications environment.
b) monitoring the use of IT resources to ensure compliance with corporate policy and procedures.
c) providing user manuals and other appropriate user tools for independent study by user departments where appropriate.
d) scheduling training opportunities, on a regular basis, for all standardized applications for all user groups.
e) operating a help desk support service for user inquiries on all standard applications and acting as a consultant for systems design of new products.
f) purchasing and support of all approved desktop, laptop computers or other forms of data processing hardware, software and peripherals.
g) purchasing and support of all approved cell phones, land line phones, voicemail and hand held smart phone technologies.
h) all computer equipment installations, modifications, and relocations.
i) purchasing and supporting of all other approved technologies as covered by the I.T.S. General Use and Practices Policy and procedures.