Corporate Policy

Policy No. **03-05-01** ***Effective Date:*** **Jul 21 2009 12:00AM**

SECTION: CORPORATE ADMINISTRATION
DEPARTMENT/DIVISION FINANCE / CORPORATE INFORMATION & TECHNOLOGY
SUBJECT: **COMPUTER USE**

POLICY STATEMENT:

It is the Policy of The Corporation of the City of Thunder Bay (the City) to outline rules for Users of the City's Computer Resources on the acceptable uses of those resources. It is every Users duty to use the City's Computer Resources in a professional, ethical and lawful manner.

PURPOSE:

To outline the rules and responsibilities associated with the use of the City's Computer Resources, to protect the reputation and the Computer Resources of the City from irresponsible or illegal activities, and to ensure the privacy, security and reliability of the City's network and software applications.

DEFINITIONS:

When a term set out below appears in the text of this Policy with its initial letters capitalized, the term is intended to have the meaning set out for it in this section. Wherever a term below appears in the text of this Policy in regular case, it is intended to have the meaning ordinarily attributed to it in the English language.

(a) "City" means The Corporation of the City of Thunder Bay.

(b) "Computer Resources" refers to the City's entire computer network, including: all hardware, software programs, applications, e-mail and internet systems, data, information and other work products installed or created through the use of these tools.

(c) "Offensive Material" means material that is obscene or pornographic (including sexually explicit material, nudity, sexually explicit jokes, sexually degrading material), racially offensive or degrading, defamatory, discriminatory, or hate propaganda.

(d) "Personal Time" is defined as time at lunch or coffee breaks, or time before or after regular work hours, and not during paid overtime .

(e) "Policy" means this policy, including related procedures as set out herein.

(f) "User" refers to all employees, agents, independent contractors, consultants, students, volunteers, elected officials, and any other person or entity who use the City's Computer Resources with authorization.

(g) "Legally owned software" means proof of legal ownership can be produced otherwise it is considered illegal. Any of the following can serve as proof of ownership:

The original license for the software package.
A purchase order for the software package.
A cheque request for the software package.

An original CD with a serial number for the software package.
Proof of purchase from the vendor.
Vendor documentation for free downloads.

In using the City's Computer Resources, Users must comply with this Policy.

1. All Computer Resources are the property of The City and may be used only for legitimate business purposes. Authorized Users are permitted access to Computer Resources to assist them in the performance of their duties to conduct City business only.
Information or data cannot be copied to removable media for, or downloaded electronically to, other individuals or entities for any purpose other than approved City business. Should a User have any doubt as to the appropriateness of a request for such information or data, the advice of his or her Division Manager must be obtained before proceeding.

2. Electronic documents related to City business, including e-mails, that are created, sent, received and retained by a User either electronically or on paper and placed in a paper file, are considered to be the records of the City and as such are subject to all of the access and privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act and the Records Management Policy (Policy No. 03-06-01).

3. The City's Computer Resources cannot be used for any activity for which a User receives remuneration or 'in-kind' service or other financial benefits other than those received directly from the City, whether during work hours or on Personal Time.
4. User-ID/passwords must be confidential to each User and are not to be shared amongst Users (except for Corporate Information & Technology pre-arranged group user IDs). Users must access the City's Computer Resources using his or her ID/passwords and no User may access the Computer Resources using another User's ID/passwords.
Users are responsible for all activities that occur under their ID/passwords. Users are responsible for immediately reporting any known or suspected compromise of their ID/passwords. If an irregularity is suspected or reported, Corporate Information & Technology can access and examine logs to determine if unauthorized usage may be occurring.
Users are responsible for safeguarding their ID/passwords. ID/passwords must not be written down or stored on-line unless adequately secured. ID/passwords must not be easily accessible to others (e.g. taped to the computer, under a keyboard).
ID/passwords should be easy for the User to remember and difficult for others to determine. Password length must be nine characters or more, made up of a combination of characters, numbers and special characters (e.g. 9AmZfive!), not composed entirely of words or people's names.

5. Incidental and occasional personal use of the City's Computer Resources is allowed on a User's Personal Time, provided such use will not result in any measurable expense to the City in time or materials, and provided such use does not violate any aspect of this Policy. Users shall not store files not related to City business on the City network.

6. Permanent information is not to be stored on individual computers or any external storage medium. Information or data, source code and programs, where applicable, are to be stored on the network server rather than the local hard drive so that appropriate protections and backups can be provided on a regular schedule by Corporate Information & Technology. Where external storage mediums are required, authorization must be obtained from the User's Division Manager prior to use.

7. Only hardware and software that have been approved by the Manager of Corporate Information & Technology are to be used on the City's Computer Resources. Software and hardware are not to be added or removed from the City's Computer Resources without prior

approval or in consultation with the Manager of Corporate Information & Technology.
All software on computers must be legally owned and used in accordance with the license and copyright agreements for the specific software in use.

8. The Computer Resources provided to Users are to assist them in the performance of their duties. Users do not have privacy, nor should they have an expectation of privacy, in anything they use, create, store, send, or receive. All Computer Resource activity is subject to random inspections or audit by the City. The City may monitor, access or audit a User's use of Computer Resources on a periodic basis to assess compliance with this Policy, including: User activities, Internet usage, e-mail usage, and all saved files (including archived material of present and former Users), without the User's consent or knowledge, and notwithstanding any confidential or personal designation. Automated audit and logging tools are used for monitoring all network activity whether it is for business or incidental personal use.

9. The City's Computer Resources are not intended for personal use and Users (past and present) must not have any expectation of privacy when using Computer Resources for personal use. All electronic communications are considered to be the records of the City, and shall be subject to the Municipal Freedom of Information and Protection of Privacy Act and any restrictions placed upon their use by the City or by the sender of the communication.

10. If a sensitive or confidential e-mail is sent to the wrong person, the Manager Corporate Information and Technology, after receiving approval from the City Manager, City Solicitor, General Manager Finance, or designate, may remove the e-mail from the receiver's inbox without the receiver's consent or knowledge.

11. Transportable equipment, including laptops, must be secured. Assigned Users of the devices must ensure their proper security at all times.

12. All Users have a responsibility to report violations of this Policy to their immediate supervisor or to the Manager Corporate Information & Technology.

REMOTE ACCESS:
Remote access (including dial-up and Virtual Private Network (VPN) is granted to Users for the purpose of conducting City business outside of the office workplace. This access must be approved by the Division Manager of the User. Elected officials require the approval of the C ity Manager .

It is the responsibility of Users with remote access privileges to take all reasonable care to prevent the use of the remote connection by non-Users to gain access to the City's Computer Resources. The User must take all reasonable care to protect the City's Computer Resources.

At no time are Users to provide their login usernames and/or passwords to anyone, including family members.

INTERNET USE:
Certain Users may be provided with access to the Internet to assist them in the performance of their duties. Internet access is provided to those Users for research or operational support purposes relevant to the City's business.

The User's immediate supervisor is responsible for the User's use of the Internet. Division Managers may request that public Internet access for their specific User and/or locations be unblocked.

The User's immediate supervisor, Manager Corporate Information & Technology, along with the Manager Human Resources, will co-ordinate any action as a result of abuse of Internet privileges.

Personal use of the Internet is allowed during the User's Personal Time as long as it does not interfere or conflict with business use and this Policy, and provided the User has his or her supervisor's approval.

Under no circumstances is the Internet to be used to access sites that generally are viewed as inappropriate, including sites containing Offensive Material.

Any exception would require the express authorization of the department General Manager and Manager Corporate Information & Technology for the purpose of work-related research.

Users shall not under any circumstances use the Internet for illegal purposes, or to gather information to support illegal activities.

Downloading of non-executable files (including but not limited to reports, spreadsheets and information flyers) for business use is permitted. Users must exercise reasonable care that the file's source is reliable to avoid the introduction of viruses.

E-MAIL AND E-MAIL SYSTEM USE:

Corporate Information & Technology will automatically and permanently destroy all e-mails that are older than 365 days and have not been properly stored in accordance with the Records Management Policy (Policy No. 03-06-01).

E-mails are corporate records of the City. Professional business practices shall be adhered to by Users in the creation and content of all e-mails. Confidential corporate information can be communicated on the email system by Users. Other text or information that is not suitable for release to the public must not be included in e-mails.

The City's e-mail system cannot be used by Users to send any Offensive Material.

Users are prohibited from monitoring, intercepting or tampering with another User's e-mail communication, except as authorized by this Policy.

The sending of business related e-mail from a User's personal account to City clients is prohibited.

MANAGEMENT OF USERS:

Managers/supervisors will notify Corporate Information & Technology - Network & Technology Services of all changes to be made to their employees' User ID, including: disabling the User's access (temporarily or permanently), deleting the User ID, adding new Users, changing access rights, advising of User location changes.

Upon termination or transfer of a User's duties, all data and information are to be turned over to the User's direct supervisor for retention and then deleted from the User's hard drive, especially e-mails saved under the Lotus Notes series folders. Direct Supervisors will have 30 days to review the mailbox of terminated or transferred employees. No information is to be deleted or otherwise made inaccessible or non-functional regardless of storage medium. All information is confidential to the User's department and remains the property of the City.

POLICY VIOLATION:

Any breaches of this Policy will be reviewed and may result in corrective or disciplinary action up to and including dismissal.

Any Computer Resources found to be in violation of this Policy may be removed, deleted, confiscated or altered.

For the purpose of considering corrective or disciplinary penalties as a result of computer use Policy violations, the City has zero tolerance for violations relating to the knowing or intentional viewing, accessing, downloading, storing or distribution (via e-mail, hardcopy, images, text, video-clips, or otherwise) of Offensive Material. These violations will be considered a serious infraction.

The Manager Human Resources, the User's Division Manager along with the Manager Corporate Information & Technology will investigate alleged breaches of this Policy and determine whether the User's access will be temporarily suspended during the investigation. Where a breach is substantiated, a record of the investigation and any corrective or disciplinary action taken will be placed in the User's personnel file.

REFERENCE:

The Ontario Human Rights Code
The Criminal Code of Canada
Municipal Freedom of Information and Protection of Privacy Act
City of Thunder Bay Retention Bylaw
Records Management Policy No. 03-06-01
Disciplinary Process Policy No. 06-01-07
Responsible Use of Email Procedure
Corporate Report 2009.099
Securing Your Corporate Blackberry Device Procedure
Information Technology - Mobile Devices Procedure

Approved By: City Council **Date:** Jul 21 2009 12:00AM

Replacing/Amending: 14/05/2001

Originating Department: Finance

Contact: Manager, Corporate Information and Technology

Departmental Procedures Manual: Yes

Affected Departments: