SECTION:	CORPORATE INFORMATION TECHNOLOGY
DEPARTMENT/DIVISION:	CORPORATE SERVICES / CORPORATE INFORAMTION TECHNOLOGY
SUBJECT:	**ACCEPTABLE COMPUTER USE**

POLICY STATEMENT

It is the policy of The Corporation of the City of Thunder Bay (the City) to outline acceptable use of the City's IT Resources. Every User has a duty to use the City's IT Resources in a professional, ethical, and lawful manner.

PURPOSE

The purpose of this policy is to outline the roles and responsibilities associated with the acceptable use of the City's IT Resources; to protect the reputation and the Information Technology 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" refers to The Corporation of the City of Thunder Bay.

(b) "CIT" or "Corporate Information Technology" refers to a Division of the Corporate Services Department within the City of Thunder Bay.

(c) "Electronic Records" are data or documents that are stored on an electronic device, either saved to a server network or within the device, including but not limited to: word processing files, spreadsheets, PDFs, data, source code, programs, web content systems, internally developed applications, and emails.

(d) "IT Resources" refers to the City's entire Corporate Information Technology infrastructure attached to the corporate network, including software programs, all hardware including desktops, laptops, smartphones, tablets, peripheral devices, POS (point of sale) devices, email and internet systems, data, information, and other work products installed or created using these tools whether active or archived. This also includes transmission methods and services such as wired and wireless networks.

(e) "Non-Executable Files" are files that cannot be executed directly by the processing system. Non-Executable Files are created for a specific task. Examples include PDFs, spreadsheets, and Word documents.

(f) "Offensive Material" refers to material that is obscene, sexually explicit or degrading, racially offensive or degrading, defamatory, abusive, harassing, threatening, discriminatory, fraudulent or hate propaganda.

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

(h) "Policy" refers to the Acceptable Computer Use Policy (03-05-01), including related procedures as set out herein.

(i) "User" refers to all employees, elected officials and students and any other person or entity who use the City's IT Resources with authorization.

(j) "Quarantine" refers to the act of blocking or withholding messages sent or received via email that have been detected as potential spam or malicious content.

CONDITIONS

1. All new employees must read this Policy and sign the Computer Use Acknowledgement form when initially hired through Human Resources.

2. All IT Resources are the property of the City. The intended use of these resources is to perform City business.

3. Information or data cannot be replicated, downloaded, printed, or shared for any purpose other than approved City business. Concerns regarding the appropriateness of a request for such information or data should be directed to the Division Manager and/or the Office of the City Clerk.

4. Electronic Records created and stored on IT Resources, including emails, that are created, sent, received, and retained by a User electronically, are considered records of the City and are subject to all the access and privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act and the Records Management Policy (03-06-01).

5. The City reserves the right to access IT Resources used by Users under any of the following conditions:
    a. to engage in technical maintenance, repair, and management;
    b. to meet a legal requirement;
    c. to produce records, including e-discovery;
    d. to ensure continuity of work processes (for example, employee departures, leaves of absences, or work stoppages);
    e. to improve business processes; and/or
    f. to investigate misconduct and ensure compliance with the law.

6. City IT Resources cannot be used for any activity for which a User receives remuneration, 'in-kind' services, or other financial benefits other than those received directly from the City, whether during work hours or on Personal Time.

7. Incidental and occasional personal use of the City's IT Resources is allowed on a User's Personal Time, provided such use will not result in any measurable expense to the City and that such use does not violate this Policy.

8. The use of IT Resources on Personal Time does not afford Users privacy during that period of use.

9. Users shall not store files unrelated to City business on the corporate network. CIT reserves the right to remove personal files without prior consent from Users.

10. To ensure appropriate backups as outlined in the Data Backup and Recovery Policy, Electronic Records are to be stored on a network repository rather than the local hard drive to maintain security and conduct backups.

11. Information or data are not to be stored externally for extended periods of time. Use of external storage is appropriate when required to present work outside of your traditional workstation.

12. Where external storage mediums are required for extended periods of time, it must be encrypted to the satisfaction of CIT and authorization must be obtained from either the User's Division Manager, Director – Corporate Information Technology or designates prior to use.

13. All IT Resource activity is subject to logging, random inspections, or audits by the City.

14. Only approved hardware and software are to be used with City IT Resources. No modifications to hardware and software are permitted without prior approval from CIT.

15. All software is to be used in accordance with its license and copyright agreements.

16. Users shall not under any circumstances use IT Resources for illegal purposes or to gather information to support illegal activities.

17. All Users have a responsibility to report violations of this Policy to their immediate supervisor.

NETWORK USER IDENTIFICATION (USER ID)

1. Passwords are enforced based on the complex rules and expiry dates as defined by CIT.

2. When Users request support for unlocking accounts or password resets, they must identify themselves and validate access. Users will authenticate based on CIT validation processes.

3. Passwords are confidential and are not to be shared amongst Users. Users are responsible for safeguarding their passwords.

4. In accordance with the Remote Access Policy, 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 IT Resources. The User must take all reasonable care to protect the City's IT Resources.

5. Users are responsible for all activities that occur under their User ID/password.

6. Users are responsible for reporting any known or suspected compromise of their User ID/password.

INTERNET USE

1. Under no circumstances is the internet to be used to access sites that are viewed as inappropriate, including sites containing Offensive Material. Users shall not under any circumstances use the Internet for illegal purposes, or to gather information to support illegal activities.

2. 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 SYSTEM USE

1. Emails stored in User's mailboxes older than 365 days and that have not been properly filed in accordance with the Records Management Policy (03-06-01) will be automatically and permanently destroyed.

2. The City reserves the right to filter and Quarantine both inbound and outbound emails to ensure the confidentiality and security of IT Resources.

3. The City's email system is not to be used by Users to send any Offensive Material.

4. Emails sent from Users for City business must follow Canada's Anti-Spam Legislation (CASL) guidelines.

5. The Director - Corporate Information Technology or designate may instruct CIT staff to remove a sensitive or confidential email mistakenly sent to the wrong person without the recipient's consent or knowledge.

MANAGEMENT OF USER ACCOUNTS AND IT RESOURCE ACCESS

1. Managers/Supervisors will notify CIT 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, and advising of User location changes.

2. Upon termination or transfer of a User's duties, the User's direct Supervisor or designate will receive access to email and Electronic Records for retention and access purposes. All information is confidential to the User's department and remains the property of the City and responsibility of the Supervisor, as per the Records Management Policy.

POLICY VIOLATION

1. Alleged breaches of this Policy will be investigated by the Director – Human Resources, Director – Corporate Information Technology, and the User's Manager, or designates.

2. The User's access may be temporarily suspended during the investigation at the discretion of the parties investigating the alleged breach.

3. Any breaches of this Policy are subject to disciplinary action. Where a breach is substantiated, a record of the investigation and any corrective or disciplinary action taken will be placed in the User' personnel file.

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

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

SCOPE

This policy applies to City employees and Users of IT Resources, including the use of information, computer devices and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by the City.

REFERENCE

The Ontario Human Rights Code
The Criminal Code of Canada
Canada's Anti-Spam Legislation, S.C 2010, c.23
Municipal Freedom of Information and Protection of Privacy Act, R.S.O 1990
Data Backup and Recovery Policy 03-05-02
Conflict of Interest Policy (06-01-05)
Code of Conduct for Employees (06-01-38)
Disciplinary Process Policy (06-01-07)
Mobile Device Policy 03-05-05
Records Management Policy (03-06-01)
Remote Access Policy (03-05-06)
Violence in the Workplace (06-01-37)
Workplace Harassment and Discrimination (06-01-32)
Disciplinary Penalties Procedure (HR-05-03)
Electronic Monitoring Procedure (HR-05-36)

APPROVED BY:	City Council	***Date:***	March 25, 2024
Replacing/Amending:	2001.124		
Originating Department:	Corporate Services/Corporate Information Technology		
Contact:	Director, Corporate Information and Technology		
Departmental Procedural Manual:	Yes		
Affected Departments:	All		