Technology Usage Policy

Section	Date	Bylaw Number	Page	Of
Human Resources	February 18, 2020	28-2020	1	5
Subsection	**Repeals By-Law Number**		**Policy Number**	
General	142-2010		HR-2-6	

Policy Statement
The City of Kenora provides Information Technology systems and devices to employees and members of Council in order to support and improve City services. The use of these systems and devices for personal benefit is a privilege given by the City of Kenora and employees are encouraged not to abuse this privilege.

Purpose
The purpose of this policy is to establish standards and expectations for the appropriate use of City of Kenora Information Technology (I.T.) systems and devices.

Scope
This policy applies to all City of Kenora employees, Council members, and to anyone who has direct or remote access to the City's information technology infrastructure.

Definitions
Data – any document, email, or message generated by a person using the City's hardware or software in any application

I.T. Systems and Devices – all electronic communication systems, data, internet, applications, computing systems, and resources owned or leased by the City of Kenora including but not limited to computers, laptops, tablets, radios, cell phones, smart phones, email, telephones, software, messages, printers, photocopiers, and any other networked wired or wireless equipment intended to provide access to City networks, systems, or software

Roles & Responsibilities
Senior Leadership Team members are responsible for understanding and upholding this policy in addition to complying with all other applicable legislation, regulations and City policies and procedures.

Supervisors are responsible for determining which systems and devices their employees require and advising the I.T. department; any costs or budgeting considerations associated with acquiring systems and devices for their employees; monitoring their employees usage and determining the consequences of inappropriate use as per this policy; and regularly communicating and reviewing this policy with employees.

Employees are responsible for all activities under their network, email, voicemail, applications or any other such accounts; protecting their accounts and the City network from access by anyone other than themselves; reporting any violations of this policy to their Supervisor; and utilizing City IT systems and devices in an acceptable and ethical manner as per this policy.

IT Department is responsible for purchasing and acquiring all IT equipment, software and devices; ensuring account documentation is properly authorized and completed prior to issuing equipment and access to employees; and creating and installing all user accounts, access levels, systems, and software.

Prohibitions

City employees are prohibited from using the City's I.T. systems and devices for illegal or unprofessional activities including but not limited to:

- Unauthorized dissemination of confidential or proprietary City documents or information;
- Dissemination of information or data restricted by any applicable provincial or federal laws or regulations;
- Dissemination, including printing of copyrighted materials, articles or software, in violation of copyright laws;
- Destroying, altering, dismantling, preventing rightful access to or otherwise interfering with the integrity of City computer-based information and/or information resources without authorization;
- Expression of opinions that are or would reasonably appear to be on behalf of or representing the City, unless authorized to do so;
- Installation or downloading of illegal content or unapproved software;
- Forwarding of electronic messages without legitimate business purpose;
- Any use that contravenes existing Municipal, Provincial, or Federal laws or regulations.

In addition, any use that may be disruptive, offensive to others, or discriminatory as defined by the *Human Rights Code* is also prohibited. Such unauthorized use includes but is not limited to:

- Creating, accessing, sending, uploading, downloading, posting or saving language or material containing ethnic slurs, racial epithets, or anything that may be construed as threats, defamation, slander, harassment or disparagement of others based on their race, ancestry, colour, citizenship, creed, sex, sexual orientation, age, disability, gender identity, gender expression, marital or family status, religious or political beliefs;
- Sending or soliciting sexually oriented messages or images;
- Intentionally or knowingly visiting websites that have offensive content;
- Sending chain letters

Privacy and Monitoring

Employees should have no expectation of privacy as all files, documents, messages and electronic communications created on, generated by, stored on, or transmitted through the City's I.T. systems and devices are deemed to be the property of the City.

As the City is subject to the provisions in the *Municipal Freedom of Information and Protection Privacy Act (MFIPPA*), the City of Kenora reserves the right to access, inspect, and log the use of all I.T. systems and devices without notice. In addition, the City will monitor its I.T. systems and devices for security breaches, violations of law, or infringement of City rules and policies.

Business & Personal Use

The City's I.T. infrastructure is intended to be used for conducting City business. Use of the City's IT systems and devices for personal use during working hours is discouraged. Although incidental personal use is understood, this privilege should not be abused and such personal use should be brief, infrequent, and not interfere with the employees regular duties.

Using Computer systems and peripherals and Internet connections shall not be used for personal gain or profit or for the benefit of other persons or entities or for sales or personal purchases or for posting advertisements for private money making schemes including pyramid schemes.

Any costs incurred by employees through their personal use of City I.T. systems and devices not related to City business must be reimbursed by the employee to the City.

Security Measures
All employees are responsible for the security of the City's information technology and will safeguard all passwords, authorization codes, and confidential data by taking full advantage of the security mechanisms built into the City's IT systems and devices.

Employees should avoid using obvious passwords and must keep them strictly confidential. If the confidentiality of an employee's password is breached, the employee should change it immediately.

Mobile devices with access to City email accounts or information must have the minimum locking security requirements of the device such as passcodes and screen locks.

The City reserves the right to revoke an employee's access to email, voicemail, internet, and any communication systems or devices at any time, with or without cause or notification, at the City's sole discretion.

Lost or Damaged Equipment
Loss, damage, or theft of a technological device or system must be reported immediately to a Supervisor and to the I.T. department.

Policy Violations
Violations of this policy will be subject to the City's Progressive Discipline Policy up to and including termination. Where applicable, the City of Kenora may also take legal action in accordance with the law.

Related Documents
Progressive Discipline Policy HR-2-03
Vehicle Operation Policy HR-2-04
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

A signed copy of this policy shall remain on the employee's personnel files, indicating that they have reviewed, understood, and agreed to comply with this policy.

This policy has been reviewed with me. I understand the policy and agree to abide by it.

_____ _____

Date Employee Signature

_____

Print Name