POLICY NO.: **G.G 6.20**

SECTION: **GENERAL GOVERNMENT - HUMAN RESOURCES**

TITLE: **ACCEPTABLE USE OF INFORMATION TECHNOLOGY**

ADOPTION DATE:

REVISION DATE:

PURPOSE:

The purpose of this policy is to outline the acceptable use of information technology for municipal employees, council members, guests, and service providers. Inappropriate use exposes the organization to risks including malware attacks, compromise of network systems and services, loss of confidential information and legal issues.

The Municipality of Kincardine (“Municipality”) will identify responsibilities and requirements of all technology users and provide guidance for the use of corporate computers, laptops, and related components, technologies and supporting software and hardware. Through this policy, the Municipality will also communicate how and when an employee will be monitored and establish procedures related to electronic monitoring of IT assets.

SCOPE:

All employees - full-time, part-time, casual, contract, students, firefighters and members of Council - who are authorized to use corporate computers and related equipment, software, and programs, will comply with the policy.

This policy applies to all municipal sites including the Municipal Administration Centre, the Davidson Centre, the Water Treatment Plant, Fire Stations, the Waste Management Centre, the Emergency Operations Centre, all Operations sites and buildings, and all other Municipally owned sites and buildings. This policy will also apply to employees who are working remotely using corporate devices or systems.

DEFINITIONS:

Electronic Information and Technology Systems - any device or service that is utilized to create, modify, transport, or transmit any form of information in a digital format

Electronic Monitoring - using technological, electronic, or digital means to track, observe, or monitor employee actions

Service Providers - any contracted worker/company employed by the Municipality to provide a service or function as per the terms of the contract

Spamming - refers to sending an annoying, unnecessary, false, or leading message to any number of users

Trolling - creating discord on the internet by starting quarrels or upsetting people by posting inflammatory or off-topic messages in an online community

GUIDING PRINCIPLES:

All equipment and software programs, information and data installed or created on corporate equipment belongs to the Municipality. This includes all programs, documents, spreadsheets, databases, and methods or technologies developed using corporate equipment and/or software, while employed by the Municipality.

Confidential information or data cannot be copied to removable media or downloaded electronically to another individual, agency, public or private corporation, for any purpose other than approved business.

All electronic documents related to the Municipality, including emails that are created, received, and retained by an employee either electronically or on paper, are considered to be records of the Municipality and as such are subject to all of the access and privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act.

Equipment and software cannot be used for any activity for which an employee receives remuneration or “in-kind” service or other personal benefits other than those received directly from the Municipality.

Incidental and occasional personal use of corporate equipment and software is allowed, similar to occasional use of the Municipality’s telephones, providing such limited use will not result in any measurable expense to the Municipality in time or materials.

Employee use of Municipal electronic systems including but not limited to equipment, hardware, software, data, databases, internet resources (hereafter “electronic systems”) is intended primarily for activities which are necessary to the employment of the user. Municipal electronic systems are not intended for personal use and employees will not have any expectation of privacy when using any Municipal electronic system.

PROCEDURES:

Internet Acceptable Use

Internet access is provided to employees for research and communication purposes relevant to the business and to provide such information to residents and business partners. The Leadership Team, at their discretion, may choose to block public Internet access for specific locations.

Municipality-provided Internet access and email are corporate resources and are to be used for municipal business purposes. Personal use of the Internet and email is authorized within reasonable limits providing it does not interfere with or conflict with business use, and provided the employee has their supervisor’s approval. However, under no condition is the Internet to be used to access sites that generally are viewed as inappropriate.

Downloading of non-executable files for business use is permitted. These would include reports, Adobe “PDF” files, spreadsheets, etc. Employees must ensure the source is reliable as viruses can be introduced to the system through spreadsheets and other documents.

Executable files may not be downloaded without authorization from the employee’s manager. Such software, if approved, must be checked for viruses before execution. Supervisors are responsible for their respective employees’ use of the Internet. The supervisors, along with the Human Resources department, will co-ordinate any action as a result of abuse of Internet privileges.

If email is not required as a permanent record of the Municipality, it will be read and deleted from the system. If email is to be retained, an electronic copy can be retained in an electronic folder.

Email messages are like any other communications that are created to correspond with business associates and customers. As a result, professional business practices will be adhered to in respect to the creation and content of email messages.

Any person suspecting a virus, or any other concern in regards to the municipal computer system will contact the IT department.

Prohibited Activities

The following clauses apply to all municipally owned technology regardless of location, and to any technology while on Municipal premises regardless of ownership:

- It may not be used to store, distribute, post, download, or view any defamatory, abusive, obscene, profane, pornographic, sexually oriented, threatening, racially or ethnically offensive, sexist or illegal material
- It may not be used to transmit or distribute the Municipality's confidential or proprietary information in a manner that would constitute negligence
- It may not be used for any unlawful activity as outlined in *Appendix A*
- Transmission and use of any unlicensed software, software having the purpose of damaging computer systems or files (e.g. computer viruses), software that compromises the integrity of the systems (e.g. key loggers, password sniffers) is prohibited. All software and files downloaded must be systematically checked for viruses before loading on Municipal technology systems
- Any malicious attempt to harm, destroy, or illegally access the data of any person, computer, or network linked to the Municipality's Wide Area Network (WAN) is prohibited
- The use of camera phones is strictly prohibited in private areas: locker rooms, washrooms, dressing areas, at any time. Such use may be in violation of the Criminal Code and privacy legislation and may be subject to internal and external disciplinary consequences

Software Licenses, Acquisition, Installation and Support

Only software provided by the Municipality and/or licensed to the Municipality may be installed on computer hardware that is provided by the Municipality. Unauthorized software will not be used. Any exceptions to the above require approval from the IT department.

Software will not be copied except for the sole purpose of backup. Piracy is strictly prohibited.

The Municipality will retain licenses and original copies of all licensed software. Beta versions of software and Internet downloads (including software upgrades, freeware, and shareware) must not be installed without written approval from the IT department.

Departments may request that a product be added to the corporate standard. The IT department will add that product to the list of standards where, in their judgment, the product will be of interest and benefit to the Municipality.

Management of Users

Departments must notify the IT department of all changes to be made to employee User IDs. This includes disabling the employee access (temporarily or permanently), deleting the User ID, adding new users, changing access rights, advising of employee location changes, etc.

Upon employee termination or transfer, all documentation, email, programs, etc. are to be turned over to the employee's Manager. No information is to be deleted or otherwise made inaccessible or non-functional regardless of storage medium. All information remains the property of the Municipality.

Users must surrender any documentation in their possession relating to the Municipality's hardware or software upon termination of their employment.

All User IDs and passwords are confidential to each user and are not to be shared amongst users.

Users are accountable for all activities that occur under their User ID/password. Users are responsible for immediately reporting any known or suspected compromise of their User ID/password. If an irregularity is suspected, the IT department will examine logs to determine if unauthorized usage may be occurring.

Passwords

The Municipality gives consent to employees, council members, and service providers to use domain level security authentication in accordance with the password complexity enforced at the domain level throughout the Municipality's physical and digital properties.

The Municipality is committed to ensuring that the security standards defined in this policy are regularly updated, tested, and maintained to ensure they are current and valid in compliance with best practices by the National Institute of Standards and Technology (NIST)/Communication Security Establishment (CSE).

The Municipality maintains password complexity rules at the domain level under the supervision of the IT department. The IT department will allow or deny employee, council member, or service provider access to municipal information systems at the direction, and under the supervision, of the Director of Corporate Services.

A request for new, modified, or additional access to any network device, service, software, or digital property must be submitted and approved by the Director of Corporate Services before any change will be made. The Municipality reserves the right to grant or restrict access to any portion of the internal network, systems, or devices as it deems necessary.

The following rules apply to all domain level accounts that have been authorized to access Municipally owned technology regardless of location:

- Password Length – All domain level accounts will be authenticated with a password that is a minimum of 12 characters in length
- Password Complexity – All domain level accounts will be authenticated with a password that, at minimum, consists of one uppercase letter, one lowercase letter, one number, and one special character. In addition, a password will not contain the username of the account
- Password History – All domain level accounts will have their password history restricted to one full calendar year (365 days). A password will only be usable once during this period.

Information Technology Monitoring

The Municipality reserves the right, without prior notice to the employee, guest, or service provider, to monitor the use of technology on municipal premises. Municipally owned technology provided to an employee, council member, guest, or service provider, may be accessed or recalled without any prior notice. Nothing in this policy affects or limits the Municipality's ability to use information obtained through electronic monitoring. The Municipality collects information through electronic monitoring as identified in *Appendix B.*

The right of the Municipality to access an employee, council member, guest, or service provider's e-mail, internet history, or voice mail on Municipality provided technology, or to disclose the contents, may arise in a number of situations, including:

- To comply with disclosure requests or orders made pursuant to the Municipal Freedom of Information and Protection of Privacy Act
- For Municipally owned technology, because of regular or special maintenance of the electronic information systems
- For Municipally owned technology, when the Municipality has a business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable
- In order to comply with the obligations to disclose relevant information in the course of a legal proceeding; and when the Municipality has reason to believe that there has been a violation of this policy, or the use is incompatible with the Municipality's mission as a governing body

Notice To Employees

The Municipality will provide a copy of this policy to each employee within thirty (30) calendar days of implementation. If any changes are made after its implementation, each employee will be provided a copy of the policy within thirty (30) days of the changes being made.

All new employees will receive a copy of the policy upon commencing employment and this policy will be circulated to staff on a regular basis for review. When in doubt, employees have the responsibility to seek clarification from Management.

Compliance

The Human Resources department will ensure all employees acknowledge that they have read and understood the policy (and related documentation) and will place a signed copy of the acknowledgement form in their employee file. Compliance with the policy is a condition of employment.

Failure to comply with this policy may result in the loss of access privileges, financial compensation to the Municipality, pursuance of criminal charges, and/or other disciplinary action up to and including termination.

REFERENCES:

1. Appendix A - Unlawful Information Technology Activity Examples
2. Appendix B - Electronic Monitoring Practices

ACKNOWLEDGEMENT & AGREEMENT:

I, __________________________, acknowledge that I have read, understand, and will adhere to the Acceptable Use of Information Technology policy of the Municipality of Kincardine.

NAME:	
SIGNATURE:	
DATE:	

APPENDIX A - Unlawful Information Technology Activity Examples

For the purpose of this policy, *inappropriate use* and *unlawful activity* are interpreted broadly and includes any criminal activity or other illegal activity.

Pornography	Possessing, downloading, or distributing any material deemed pornographic in nature
Intellectual Property	Infringing on another person’s copyright or trademark of any other property without lawful excuse
Other Criminal Activity	Using technology as a means to commit criminal activity (examples include, but are not limited to, fraud, extortion, sale and/or purchases of restricted goods)
Defamatory Libel	A matter published without lawful justification or excuse, that is likely to injure the reputation of any person by exposing that person to hatred, contempt, or ridicule, or that is designed to insult the person – The Libel and Slander Act, RSO 1900, Chapter L.12
Disclosing or Gathering Personal Information	Disclosing or gathering personal information in a manner inconsistent with the Municipal Freedom of Information and Protection of Privacy Act
Hacking and Other Crimes Related to Computer Systems	Examples include, but are not limited to, the following: • Gaining unauthorized access to a computer system • Trying to defeat the security features of network connected devices • Use of software and/or hardware designed to intercept, capture, and/or decrypt passwords • Intentionally spreading a computer virus • Destroying or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it • Interfering with other’s lawful use of data and technology
Harassment	Using technology, without lawful authority, to cause people to fear for their safety or the safety of anyone known to them
Hate Propaganda	Communicating messages that promote or incite hatred against an identifiable group that is likely to lead to a breach of the peace
Inception of Private Communications or Electronic Mail (In Transit)	Unlawfully intercepting someone’s private communications or unlawfully intercepting someone’s electronic mail
Obscenity	Distributing, publishing, or possessing for the purpose of distributing or publicly displaying any obscene material

APPENDIX B - Electronic Monitoring Practices

The Municipality collects information through electronic monitoring in the following ways:

Monitoring Tool	Overview	Purpose
GPS	Fleet within the municipality that perform road maintenance or monitoring are equipped with GPS units.	Allows the Municipality to confirm completion of year-round road patrols to ensure maintenance standard compliance Allows the Municipality the ability to confirm location of fleet when investigating complaints or claims
Video Surveillance (CCTV)	Cameras record video footage of specific areas of the following facilities: • Water Treatment Plant • Municipal Administration Centre • Waste Management Centre • Davidson Centre	Assists with facility security
Electronic Meetings	Council Meetings are recorded in the Council Chambers using cameras or videoconferencing technology	Allows for transparent government and effective records management
Emergency Services Applications	Utilized by volunteer Firefighters to receive notification of response calls and applicable only if tracking is enabled in the App. Only provides real-time data.	Can be utilized to identify the number of Firefighters who have responded to a call and can verify if the dispatch of additional resources is necessary
Network Access	Accessing our internal network to gain access to systems, email, files and documents. Monitoring of network access is passive – there are logs but no alert threshold	Provides information regarding authentication instances and can expose abnormal login activity
Remote Access	Accessing the municipal network from an external location. Records of login success/fail, logout and session length are monitored	Provides logs and alerts regarding authentication and can expose abnormal login activity
File Access	Accessing internal files and documents on the network based on specific permissions. Monitoring of file access is passive – there are logs but no alert threshold	Exposes security issues and provides historical data regarding creation, modification, and deletion of data

Email Access	Controls data flow to users within the network.	Provides logging and alerts that allow us to expose potential threats
Cell Phone & Tablet Use	Not currently monitored	