



Policy

Section: 3.0 Human Resources

Policy: Technology Policy

By-Law: 2022-172

Date: 17 October 2022

Revision: May 29, 2024

Coverage:

This policy shall apply to all non-union employees of the Township of Huron-Kinloss, as well as union employees subject to the terms and conditions in their respective collective agreements. Where applicable this policy will also apply to council members and committee members.

Policy Statement:

The Township of Huron-Kinloss values trust, discretion and transparency. The purpose of this policy is to ensure that all employees, elected officials, and representatives of the Corporation of the Township of Huron-Kinloss practice responsible usage of equipment and technology including email and internet. The Township recognizes the importance of mobile communication devices and wishes to establish guidelines for their consistent, convenient and cost-effective use.

Legislative Authority:

N/A

Contents:

Email, Internet & Intranet

Mobile Communications

Electronic Monitoring

Use of Generative Artificial Intelligence



Township of Huron-Kinloss

Technology Policy

Contents

- Policy..... 1
 - Coverage:..... 1
 - Policy Statement:..... 1
 - Contents:..... 1
- 1.0 Email, Internet and Intranet 3
 - GENERAL PRINCIPLES..... 4
 - 1.0 Ownership..... 4
 - 2.0 Privacy of communications 4
 - 3.0 Data security..... 4
 - 4.0 Monitoring..... 4
 - 5.0 Personal use..... 4
 - 6.0 Downloading 5
 - 7.0 Unacceptable use of Internet-related systems..... 5
 - 8.0 Education 6
 - 9.0 Enforcement..... 6
 - 10.0 Amendments 6
 - 11.0 Freedom of Information 6
 - 12.0 Disclaimer 7
- 2.0 Mobile Communications..... 8
 - Eligibility 8
 - Implementation 8
 - Program Management..... 8
 - Guidelines for Use..... 9
- 3.0 Electronic Monitoring Policy 11
 - GPS Tracking..... 11
 - Email and Computer Access..... 11
 - Access to Facilities 11
 - Generative Artificial Intelligence Tools..... 11

General.....	12
3.0 Use of Generative Artificial Intelligence Policy.....	13
Definitions:.....	13
General.....	13
Responsible Use and Ethical Use Guidelines	13
Approved use of Generative AI.....	14

1.0 Email, Internet and Intranet

“Intranet” means the Corporation’s internal website.

“Internet” means all activities undertaken through the Corporation’s Internet resources including electronic mail and browsing external web sites unless otherwise specified.

Access to Internet-related systems enables employees, agents, elected officials, and representatives of the Township of Huron-Kinloss to gather information relevant to the Corporation’s business from external sources; and to provide information to residents, potential residents, businesses and business prospects.

The purpose of this policy is to ensure that all employees, agents, elected officials, and representatives of the Corporation of the Township of Huron-Kinloss practice responsible usage of email and internet.

This policy outlines the Corporation’s requirements regarding acceptable Internet and Intranet Electronic Mail (Email) usage.

Electronic mail access is automatically provided to employees through Microsoft Outlook. Additional approval is not required.

Access to other Internet functions is determined by the requirements of the employee’s position. It is the responsibility of the Senior Management of each department to assess employee needs when granting access.

When email is used internally or externally the comments contained in the message may be viewed as an opinion of the Corporation of the Township of Huron-Kinloss and legal ramifications may result if improperly used. In order to avoid any confusions or misconceptions, email use shall be limited to work related matters only.

Email is a form of business communication and should be treated as such. Be professional in all email communications.

Remember that email messages are not confidential. If required to distribute confidential information, send it another way or make sure it is properly encrypted.

When using the Internet to conduct research or to make business-related decisions, always consider the source. Ensure that the information obtained is credible, accurate and up to date. This may require verification through an independent source.

GENERAL PRINCIPLES

1.0 Ownership

Corporate provided Internet/Intranet and Email privileges, like computer systems and networks, are considered corporate resources and are intended to be used for business purposes.

2.0 Privacy of communications

Correspondence via Internet Email is NOT guaranteed to be private. While network administration provides a high level of privacy and security on the network, users should be aware that Email messages can be recovered even though deleted by the user.

3.0 Data security

Employees must safeguard their login ID and password from disclosure to any person except the Treasurer or CAO. Users must use their own log ID and password and must immediately report any known or suspected compromise of their ID to the Treasurer or CAO.

4.0 Monitoring

The Corporation will monitor all employee usage to ensure proper working order, appropriate use by employees, and the security of corporate data. Also, the Corporation will retrieve the contents of any employee communications in these systems from time to time.

The distribution of any information through Internet-related systems is subject to the scrutiny of the Corporation to determine suitability.

Users may also be subject to limitations on their use of Internet-related resources.

5.0 Personal use

Internet and email access is provided to enable employees to perform their job effectively. Employees are expected to restrict Internet and email use to work-related activities. Although occasional personal use is acceptable, employees may only do so outside working hours and if it does not interfere with anyone else's work. Discretion must be taken when accessing the internet in areas of public access.

Employees may not use the corporation's email or internet access for personal business use.

If an employee receives Email that conflicts with any section of this policy, they must notify their Supervisor immediately. The Supervisor will notify the sender of such Email that it is not appropriate and to cease sending any further such type of Email.

6.0 Downloading

Downloading of non-executable files for business use is permitted. These would include reports, adobe PDF files, information flyers, etc., from other institutions or government agencies that may be useful to the Corporation. If in doubt, contact your Supervisor.

Executable software may not be downloaded. This type of software ends in a file extension .exe, .bat or .com and may contain viruses or other harmful code, which could harm the Corporation's network. If such a file is required, downloading must be done by the Treasurer. The file will then be checked for infection.

7.0 Unacceptable use of Internet-related systems

Communications and Internet access should be conducted in a responsible and professional manner reflecting the Corporation's commitment to honest, ethical and non-discriminatory business practice.

- Employees shall not visit Internet sites that contain obscene, pornographic, and hateful or other objectionable materials; send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Employees shall not solicit Emails that are unrelated to business activities. This includes the forwarding of jokes or chain-type letters to other employees in the office.
- Employees shall not use or permit the use of the Internet or Email for any illegal purpose.
- Employees shall not represent personal opinions as those of the Corporation.
- Employees shall not make or post indecent remarks, proposals, or materials.
- Employees shall not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the Corporation, to parties outside of the Corporation.
- Employees shall not download any executable software.
- Employees shall not intentionally interfere with the normal operation of the network, including the propagation or computer viruses and sustained high volume network traffic which substantially hinders others in their use of the network.

- Employees shall not examine, change, or use another person's files, output, or user name for which they do not have explicit authorization.
- Employees shall not perform any other inappropriate uses identified by their Supervisor.
- Employees shall not connect unauthorized equipment to the network for any purpose inconsistent with the business purpose of the Corporation.
- Employees shall not deliberately waste computer resources, including but not limited to bandwidth, disk space and printer paper.
- Employees shall not use the corporate network to gain unauthorized access to any computer system.
- Employees shall not install computer games on any municipally owned computer.

8.0 Education

To promote the efficient use and to avoid misuse of Internet/Intranet-related features, a copy of this policy statement will be distributed to all employees having access to Internet-related systems. Employees are required to familiarize themselves with the contents of this policy. Internet training sessions may be conducted in conjunction with the Treasurer. Supplemental training will be offered as technological and/or policy changes allow.

9.0 Enforcement

Employees who violate any of the guidelines set in the policy will lose their access privileges. Depending on the severity of the violation, employees may be subject to disciplinary action from written warnings through to employee termination. The Corporation also retains the right to report any illegal violations to the appropriate authorities.

10.0 Amendments

The Corporation may amend this Acceptable Use Policy from time to time as necessary. All employees with access to the Internet/Intranet-related systems will receive prompt notice of any amendments.

11.0 Freedom of Information

All electronic documents, which are created by or with the Corporation's computers or network, including Internet related systems are records for the purposes of the

Municipal Freedom of Information and Protection of Privacy Act and may be a public record for the purposes of this Act. Professionalism should be used at all times in emails as emails are classified as a document of record under the Freedom of Information and Protection of Privacy Act.

12.0 Disclaimer

The Corporation will not be responsible for any misuse of Corporate Internet/Intranet-related systems. Persons found to be misusing the Corporation's Internet/Intranet-related systems will be responsible for any costs or damages sustained by the Corporation or third party and will be obligated to indemnify the Corporation for any claim against the Corporation by a third party.

2.0 Mobile Communications

The Township recognizes the importance of mobile communication devices and wishes to establish guidelines for their consistent, convenient and cost-effective use.

Eligibility

Assigned Mobile Devices: Employees or Council members who are required to be available outside regular business hours and/or spend a significant amount of time outside of the office while performing their duties shall be eligible for an assigned mobile communication device, upon the approval of the appropriate supervisor and the Treasurer.

Department Issued Devices: Employees may be provided with a mobile communication device at the discretion of their supervisor for the purposes of being on call, emergency or occasional use, as required.

Personal Mobile Devices: Employees or members of Council who frequently use a mobile communications device while performing their duties may be eligible for a service reimbursement for use of a personal device on Township business, upon the approval of the appropriate supervisor and the Treasurer.

Implementation

The appropriate senior manager shall monitor their department issued devices distribution and use arrangements and reallocate available mobile resources as necessary to address the needs within specific functional areas.

Employees or Council members wishing to acquire an assigned mobile device or receive a service reimbursement shall complete the Mobile Communications Application (attached as Schedule "A") and submit to their supervisor for review.

The application shall be retained in the employee's personnel file and document the type of equipment, if any, assigned and the date of the return of said equipment.

The amount of the service reimbursement will be set at the discretion of the Treasurer based on the amount of business use and the comparable rates of similar services.

Program Management

Assigned Mobile Devices and accessories are considered Township property and shall be returned immediately upon request or termination of employment. The Township will assume the costs of usage, including monthly plans and the purchase of equipment. All bills shall be sent directly to the Township for payment and the Treasurer shall be

authorized to make any necessary changes to the service. Mobile devices assigned to individual employees and are used for personal use will not be considered a taxable benefit as long as the costs are part of an all-inclusive plan. Any plan overages that result from an employee's personal use will be the responsibility of the employee.

Employees who use their own personal mobile device for Township business may receive a reimbursement for the business portion only. This is not considered a taxable benefit when it is based on the service portion only. Personal Mobile Devices and accessories are considered personal property and the Township assumes no responsibility for payment of any monthly charges or repairs/replacement of equipment. All bills are the responsibility of the employee.

If an employee or Council member has been approved for a service reimbursement with respect to business use of a personal mobile device, they may redeem as follows:

- 1) Submit copies of their bill and/or proof of payment of the mobile service to their supervisor.
- 2) Once received reimbursement will be made through Accounts Payable during the appropriate cheque run.

Guidelines for Use

Mobile devices are intended for the purpose of conducting Township business. Individually assigned Township mobile devices may be utilized for personal use, but it is recognized by both the employee and the Township that this is municipal property. Mobile devices are a business communication support and staff are required to be professional in their use, in accordance with the employee code of conduct. The Township may make changes to the plan/device as necessary and may request the return of the device at any time.

Employees must realize that although personal calls made within the local calling region and under the usage limits provided by the Township plan do not result in additional charges, they do count toward the overall time limits established under the service agreement. Any overage, long distance, roaming or other charges for personal calls shall be the responsibility of the employee and shall be promptly reimbursed.

Cell phone numbers will be treated as privileged information and therefore, will NOT be provided directly to members of the public.

If you need to make or receive a call on your mobile device while driving, you must safely pull off the road and park your vehicle.

The misuse of a mobile device may result in the loss of its use by the individual and/or other arrangements may be made as deemed appropriate by the supervisor.

Reference: Schedule A Mobile Communications Application

Schedule B Mobile Communications Memorandum of Understanding

CRA Taxable Benefits – T413OE Rev. 19 Page 18

3.0 Electronic Monitoring Policy

Legislative Authority: *Employment Standards Act; Municipal Freedom of Information and Protection of Privacy Act.*

The Township of Huron-Kinloss values trust, discretion and transparency and believes employees deserve to know when and how they are being monitored. The Township does not actively monitor employees electronically, however there are opportunities where access to electronic communications and electronic monitoring may occur.

The Township can access information through electronic monitoring for a variety of reasons, listed below.

GPS Tracking

The Township has GPS tracking on many of their vehicles. The GPS tracks location, speed, whether the plow was down, salt was applied and other operational items of the vehicle. The main reason for this level of monitoring is for liability purposes and road patrol and inspections.

Email and Computer Access

The Township has access to employee's windows log in, work email and other Microsoft applications, using administrator rights. Access to employee's work emails may occur to put on an "out of office" message for unplanned absences, throughout the term of any unplanned absences, Freedom of Information requests if applicable or as deemed necessary to manage the operations of the organization. The Township does not actively monitor employee's work emails.

Access to Facilities

The Township has established guidelines surrounding electronic access to municipal facilities where available. Guidelines include specific timeframes to access facilities based on the position and access is restricted to respective facilities of the position. Employees have appropriate access to all their workplaces and facilities with the use of a single keyless remote FOB or use of a mobile app. This method allows full control on all functions and features via web-based program and tracks all events electronically.

Generative Artificial Intelligence Tools

The Township has established guidelines surrounding the use of Generative Artificial intelligence. The Township reserves the right to monitor the Internet usage, various websites and Generative AI models and staff activity on these resources. Action will be

taken if the Township suspects that Staff have used Generative AI in contrary to this policy or for any unlawful activity.

General

The Township reserves the right to change policies and procedures as required to comply with legislation.

The Township's electronic monitoring is aimed at collecting information that is related to the services provided and any personal information collected will be protected as per the Municipal Freedom of Information and Protection of Privacy Act.

3.0 Use of Generative Artificial Intelligence Policy

Legislative Authority: *Municipal Freedom of Information and Protection of Privacy Act.*

This policy establishes guidelines for the responsible and ethical utilization of Generative artificial intelligence (AI) tools by Township employees. Generative AI tools, such as ChatGPT, can enhance efficiency, however their use must align with the Township's values, regulations and data privacy standards. Generative AI tools may be employed for various tasks, such as drafting routine emails, generating reports and answering general inquiries. It is important to note that these tools are not a substitute for human judgment or decision making.

Definitions:

Generative AI - Class of Artificial Intelligence (AI) tools that create new data or content autonomously, such as text, images and videos. Data can be entered in a Generative AI tool to produce different outputs, which are often indistinguishable from human created content. Examples: ChatGPT, GPT, DALL-E2, Bing AI.

GPT - Generative Pre-trained Transformer is a Chatbot created by OpenAI. It uses large language models and data inputs to create a desired output that can be customized accordingly including such things as the language style, format, length of output, and level of detail.

Social Media - Websites and applications that enable users to create and share content or to participate in social networking. Examples include TikTok, Facebook, Instagram.

Output – The results that are produced from a Generative AI tool.

General

Generative AI technologies are a powerful set of tools that will have a significant impact on the productivity of individuals and organizations, but the use of such technologies presents legal, compliance and security risks. It is not always clear how data provided to public version of Generative AI models will be used, therefore the Township has developed this Policy to establish its decision and guidance on the use of Generative AI technologies.

Responsible Use and Ethical Use Guidelines

- Like other public exposure of data, you must always assume any data provided to a public Generative AI system can and will be used for training future Generative

AI models and will be made publicly available to other individuals and organizations on the Internet.

- Employees must not use or enter any confidential or restricted information into third-party Generative AI tools. Types of restricted information would include, but is not limited to, personal data, financial data, protected health information, resident data and Township proprietary information.
- Posting Township confidential information or proprietary information to public external website and technologies is strictly prohibited. Anything you would not post on social media or on a website should not be exposed to or shared with publicly available Generative AI tools.
- Employees who use Generative AI tools must review the outputs to ensure that they are factually accurate, complete and up to date. Since Generative AI tools do not cite sources for content there may also be copyright or intellectual property considerations. Employees are responsible for validating the output produced by Generative AI.
- Generative AI tools have been shown to produce incorrect or inaccurate information. In addition, Generative AI outputs are derived from data entered by many other users through the well-known process of model training. Township staff should carefully consider the impact of leveraging data that is generated by Generative AI, particularly data derived from public domain data sets.

Approved use of Generative AI

Use of public Generative AI is allowed for the following use cases:

- Summarizing information from public sources. This involves condensing lengthy articles, reports or data into concise, easily consumable summaries, saving time and highlighting key points.
- Theming information from public sources. Generative AI can analyze and categorize information based on themes or topics, making it easier to understand the overarching ideas or trends within large datasets or texts.
- Templating responses, for example emails, letters etc. Generative AI can create customizable templates for various forms of communication, ensuring consistency and professionalism while adapting to different contexts and recipients.
- Comparing information. Generative AI can be used to compare data sets, texts or information from different sources, identifying similarities, differences or trends which is particularly useful in research and analysis.

- Creating starting points for presentations or documents. Generative AI can generate outlines, initial drafts or ideas for presentations and documents, offering a foundation that can be further developed and personalized.
- Generating basic web content. This includes creating text for websites, blogs and social media posts.

The Township of Huron-Kinloss reserves the right to restrict Staff from using a particular Generative AI tool if the Staff member is deemed to be using the tool outside of this policy and its guidelines.