Policy Title: Acceptable Internet and E-mail Use Policy

Policy Number: CS-001-2024

Category: Corporate

Department: Corporate Services

Related Policies: Device Policy, Electronic Monitoring

Policy Approved By: Council

Effective Date: September 11, 2024

Revision Date:

Policy Statement:

Staff of the Municipality of North Grenville will be required to use internet and e-mail appropriately to perform their duties.

Purpose:

The purpose of this policy is to outline the acceptable use of information systems and computing equipment at the Municipality of North Grenville (the “Municipality”). These rules are in place to protect both the employee and the Municipality. Inappropriate use exposes the Municipality to risks, including malware attacks, compromise of network systems and services, loss of confidential information and legal issues.

Application:

This policy applies to all Municipal devices and employees. All employees with access to Municipal computing devices or information systems shall comply with this policy.

Definitions:

1. **Confidential Information:** information owned by the Municipality or entrusted to the Municipality that is not intended for sharing with the public. It includes Protected Information. Security protections must be applied to this information to safeguard its confidentiality, integrity, and availability.

2. **Protected Information**: information that is highly sensitive and that must be safeguarded in accordance with legislative or regulatory requirements. Protected Information is often subject to privacy breach notification laws and the loss of this information could have severe consequences for the Municipality. Examples include protected health information, payment card information and most forms of personally identifiable information.

Policy:

1. **General and Internet Use**

1.1. Employees shall not, under any circumstances, in their use of the Municipality's computing devices or information systems:

1.1.1. Engage in any activity that is illegal or violates the rights of any person.

1.1.2. Download or install software of any type without the authorization of the IT Coordinator or their designate.

1.1.3. Copy or distribute any copyrighted material without authorization.

1.1.4. Access the personal information of others without authorization, except as part of the employee's assigned duties.

1.1.5. Make any claims on behalf of the Municipality unless authorized to do so.

1.1.6. Associate the Municipality's name with any activity that would harm the reputation of the organization.

1.1.7. Visit websites exhibiting sexually explicit material, gambling sites, or sites related to illegal activities.

1.1.8. Visit websites that encourage discrimination or the violation of the rights of any group or individual, except in the course of authorized research.

1.1.9. Visit websites that share music or other files on a peer-to-peer basis, or otherwise share content in violation of copyright laws.

1.1.10. Engage in any activity that interferes with the ability of another organization or individual to conduct computing activities (e.g., denial of service attacks).

1.1.11. Provide information about the Municipality or its employees, clients, customers, or associates to any outside party, unless authorized to do so.

2. Personal Internet Use

2.1 Activities of a personal nature, such as non-business online shopping, access to personal e-mail, job searching, and access to personal pages of social networking sites are permitted provided that it is done on the user's own time, does not interfere with or conflict with Municipal use, and is at no cost to the Municipality.

3. Online File Sharing, Backup, and Synchronization Services

3.1. Online file sharing, backup and synchronization services, such as Dropbox, Google Drive, OneDrive, etc. are convenient ways to store and share files online, but increase the risk that Confidential Information will be inappropriately shared. The following controls must be followed:

3.1.1. Confidential Information must not be copied to or stored on any online file sharing or backup system without specific authorization from the IT Coordinator.

3.1.2. Use of online file sharing, backup and synchronization services for information that is not Protected Information is restricted to services approved by the IT Coordinator and Records and Licensing Coordinator.

4. Transmission of Confidential Information

4.1 Employees must not transmit any Confidential Information in any e-mail or via any instant messaging or chat service, except as part of their duties.

5. Authorized Storage Locations for Confidential Information

5.1. All Confidential Information shall be processed and stored within the applications authorized by the Municipality. No employee may copy any Confidential Information to any other location unless directed to do so by an authorized Municipal representative.

6. E-mail Usage

6.1 Email is an important communication tool, but also has the potential to cause damage to the Municipality. Inappropriate use of e-mail can result in the loss of sensitive or confidential data or intellectual property, damage to public image, damage to critical internal systems, and unintentional employee exposure to inappropriate content or material.

6.2 Municipal employees must not engage in any of the following:

6.2.1 Sending unsolicited e-mail messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

6.2.2 Engaging in workplace harassment contrary to the Municipality's applicable policies, in any form, whether through language, frequency, or size of messages.

6.2.3 Creating or forwarding "chain letters" or "Ponzi" or other "pyramid" schemes of any type.

6.2.4 Posting the same or similar non-business-related messages to large numbers of Internet posting sites.

6.2.5 Engaging in unauthorized use or forging of email header information.

6.3 In order to ensure proper branding and professionalism, all employees must include the standard e-signature on all e-mails sent outside the Municipality.

7. Social Media

7.1. All Municipal employees shall refer to By-Law No. 17-17, Social Media Policy, for information regarding the use of social media, both professionally and personally.

7.2. Some social media applications may be restricted by the Device Policy.

8. Remote Access and Personal Wireless Networks

8.1. No employee is permitted to install any wireless networking device that connects to the Municipality's systems without authorization from the IT Coordinator or their designate.

8.2. No employee or contractor may install any software or application that allows access to the organization's systems from a remote location without appropriate authorization from the IT Coordinator.

9. Reporting Security Incidents

9.1. All employees must immediately report the following as security incidents to the IT Coordinator:

9.1.1. Any unauthorized disclosure of Confidential Information, whether intentional or unintentional.

9.1.2. Any attempt to view or access Confidential Information by a person not authorized to view or access that information.

9.1.3. Any unauthorized attempt to gain physical access to, or install unauthorized software applications on, any server or workstation.

9.1.4. Any telephone, email, or other communication that includes an unauthorized attempt to receive or access Confidential Information.

9.1.5. Any unusual computer behavior (e.g., unusual error messages, unusual pop-up windows, website redirection, etc.). When unusual computer activity is observed, the computer should not be turned off to preserve valuable evidence.

10. Protecting the Organization from Cyber Threats

Sooner or later, the Municipality may be the target of an attempt to trick employees into disclosing Confidential Information or installing malicious software on Municipal systems; these are referred to as phishing or social engineering attacks. Be aware that social engineers often conduct extensive research in preparation for their attacks and may present you with names, events, or other information that you would not expect to be known to anyone outside your organization. Be aware of the following considerations:

a) Exercise caution with email attachments and links in email messages. If the message is unexpected or if you have any doubt about whether it is genuine, do not reply to the email. Contact the sender using contact information you have previously recorded.
b) Be suspicious if anyone asks you for a password, account information, or other Confidential Information. Phishing email messages can be made to look exactly like legitimate messages you have received in the past.
c) Never send Confidential Information, enter passwords, or provide account information over an insecure connection. A secure connection will always start with https:// in the browser address bar.
d) Do not click on banner ads or the ads along the top, sides, or bottoms of web pages. These ads are designed to be tempting, but some may link to malicious websites.
e) Understand that you may be targeted by cyber-criminals and that they want to steal Confidential Information from organizations. Be constantly vigilant.

11. Violations

11.1. Any violations of this policy may result in disciplinary action, which may include, but not be limited to, immediate termination of employment and/or such other legal actions as may be warranted in the circumstances.

Responsibilities:

Director of Corporate Services

- Shall be responsible for ensuring implementation of all items listed in the Policy section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Users

- Shall be responsible to:
  - Ensure that they use the Municipality's information systems and computing equipment in accordance with the policy.
  - Access IT resources in a responsible and informed manner.
  - Respect federal and provincial legislation and regulations and Municipal policies and procedures.
  - Take reasonable measures to control the use of their password, user identification and computer accounts.

- Report any incidents that may raise security concerns, including instances of viruses, spam, hacking, or any release of Confidential Information to the IT Coordinator and their Director as appropriate.

Compliance:

All Municipal staff must review and sign that they acknowledge the policy upon hiring and annually thereafter.

Policy Communication:

The policy will be shared with municipal staff upon hiring and annually thereafter.

Related Documents/Legislation:

Authorization:

This policy was authorized by Council by resolution C-2024-267 at the meeting held on September 11, 2024.

Revision History

Document Owner	Revised Date	Reason for Changes

Contact:

Any questions or concerns regarding this policy shall be directed to the Director of Corporate Services.