POLICY IT-07-001

Municipality of the County of Kings

Acceptable System & Network Usage Policy

Policy Category	Information Technology	**Most Recent Amendment**	December 7, 2021
First Council Approval	June 5, 2012	**Future Amendment Date**	September 2025

1. **Purpose**
   The Municipality of the County of Kings (Municipality) recognizes the essential role of technology in productivity, communication, and effective provision of services to the public. As such, it is critical that the Municipality's information systems, network hardware, and software are used appropriately so that integrity is maintained, and that data is secured against breach, unauthorized use, or corruption. Adherence to this Policy will reduce to the Municipality and authorized users, prevent unlawful and unethical usage, and protect the privacy of citizens and of organizations which do business with the Municipality.

2. **Scope**
   This Policy applies to all authorized users of the Municipality's technology and network services, including: all staff, including temporary and contract employees, volunteers, students, and interns; elected officials; and other organizations or individuals as authorized.

   This Policy does not apply to the use and maintenance of technology not owned by the Municipality.

3. **Definitions:**
   3.1 **Network**: a collection of systems interconnected by communication channels that allow sharing of resources and information; includes connectivity to the Internet where applicable.
   3.2 **Peripheral**: means a device attached to a host system, but not part of it, which is generally dependent on the host; it expands the host's capabilities but does not form part of the system's core structure. Common Peripherals include, but are not limited to: printers, fax machines, digital cameras, data storage devices, projectors, keyboards, speakers, and monitors.
   3.3 **Software**: the entire set of programs, procedures, and routines associated with a system.
   3.4 **System**: a communication device designed to accept data, perform prescribed mathematical and logical operations at high speed, and display the results of these operations; such devices include computers, e.g., desktop, laptop, tablets, mobile devices, and telephones.
   3.5 **Users**: all individuals authorized to use the Municipality's technology and network services as specified in the Scope of this Policy.

4. **Policy Statements**
   Acceptable Usage
   4.1 The Municipality's systems and network must be used primarily to conduct the business of the Municipality. In recognition of the need to occasionally attend to personal matters during work hours, reasonable personal use of systems is allowed, provided that it does not interfere with municipal business.

4.2 Users shall follow all applicable Provincial and Federal laws governing the use of systems. This shall include, but not be limited to the use of portable systems, e.g., mobile phones and tablets, while operating municipal vehicles or private vehicles in the conduct of municipal business.

4.3 The following activities while using municipal systems and the network are strictly forbidden:
- 4.3.1 Propagation of any virus, worm, Trojan horse, or trapdoor program code;
- 4.3.2 Disabling, defacing, or overloading any computer system or network;
- 4.3.3 Circumventing any system intended to protect the privacy or security of the network or another User either internally or externally;
- 4.3.4 Misuse of municipal assets or resources, harassment of any kind, unauthorized public speaking, violating confidentiality, and misappropriation of intellectual property;
- 4.3.5 Downloading or distributing pirated software or data; and
- 4.3.6 Engaging in any communications that are libelous or slanderous, or which promote, foster, or perpetuate discrimination on the basis of race, creed, colour, age, religion, gender, marital status, physical or mental disability, or sexual orientation.

Appropriate content

4.4 The following are categories of websites prohibited from access which shall not be visited by users under any circumstances:
- 4.4.1 File sharing sites not authorized for use by the Manager of Information Technology;
- 4.4.2 Piracy sites;
- 4.4.3 Sites that promote, foster, or perpetuate discrimination on the basis of race, creed, colour, age, religion, gender, marital status, physical or mental disability, or sexual orientation;
- 4.4.4 Sexual content and sites that link to sexual content, and;
- 4.4.5 Sites that are illegal or promote illegal activities contrary to the laws of Canada, the Province of Nova Scotia, or other jurisdictions, if applicable.

4.5 Users who discover they have accidentally connected to a website described in section 4.4 or other potentially offensive material, must immediately disconnect from the website and notify a Network Administrator of the occurrence.

Representing the Municipality

4.6 As any written communication could be interpreted as representing opinions of the Municipality, users must ensure they maintain the clarity, consistency, and integrity of the Municipality's mandate and image when using municipal systems and the network to conduct business on behalf of the Municipality.

4.7 With respect to sharing information online:
- 4.7.1 Only those users who are authorized to speak to the media or publically on behalf of the Municipality may speak or write in the name of the Municipality;
- 4.7.2 Other users may participate in the course of business when relevant to their duties, but must do so only as individuals speaking for themselves. In doing so, they must not reveal confidential information, customer data, trade secrets, and any other material covered by existing municipal policies and procedures.
- 4.7.3 Where an individual participant is identified as an employee or agent of the Municipality, that person must refrain from political advocacy and the unauthorized endorsement, or appearance of endorsement, by the Municipality of any commercial product or service not sold or serviced by the Municipality.

Corporate Email Distribution Lists

4.8 The use of corporate email distribution lists are controlled to ensure they do not overburden network resources and are used only for their intended purpose. The inappropriate use of corporate email distribution lists may expose the Municipality and others to significant liability and reputational risk. To mitigate this risk:

4.8.1 each distribution list must have a clearly defined purpose which is understood by all users;
4.8.2 one user is assigned to administer a list to ensure it is kept up-to-date and that its purpose continues to be relevant; and
4.8.3 users must ensure that the intended recipients in a corporate email distribution list are suitable given the purpose of the email being sent.

Safety & Security

4.9 Users shall not make changes to or disable software which has been installed on municipal systems or the network for the purpose of protecting users and the Municipality's privacy and security, or protecting municipal systems and the network against viruses and malicious software.
4.10 To avoid introducing viruses and malicious software to municipal systems or the network, users must not connect portable storage media to municipal systems or the network other than those provided by IT staff.
4.11 When connecting to other systems by any means, users are expected to understand the source and use care when downloading files from outside the network.
4.12 Users will not attempt to disable, defeat, or circumvent any security facility including the Municipality's Internet firewall.
4.13 Files containing sensitive or private data that are transferred over the Internet must be transferred using a VPN client or other encryption software.
4.14 Users are prohibited from downloading and installing non-standard software on municipal systems and connecting peripheral devices to systems on the network without approval from IT staff.
4.15 Server rooms are restricted areas and can only be accessed by IT staff or outsourced technical support services.

Freedom of Information and Protection of Privacy (FOIPOP)

4.16 All users shall adhere to duties and requirements established by Freedom of Information and Protection of Privacy legislation as detailed in Part XX *Municipal Government Act*.
4.17 Activity records for individual system and network usage, including, but not limited to, call history, emails, text messages, and Internet access, is information that the Municipality may be required to release to the public, if requested, under FOIPOP.
4.18 All users must use only authorized means to access the network and their municipal email account to conduct any and all business of the Municipality. Use of unauthorized systems and networks for municipal business could make those systems and networks subject to access in the event of a request made under FOIPOP.
4.19 Users shall take care when e-mailing non-users to ensure that all recipients of the e-mail have a right to know the provided information, and that personal privacy is protected. This may include the need to use the bcc function of e-mail to avoid unintended disclosure of recipient e-mail addresses.

Personal Accountability

4.20 Prior to gaining access to the municipal system and network for the first time, all users are required to sign the *Municipal Information System and Network User Agreement*, attached to this Policy as Schedule A, indicating that they have read, understand, and agree to abide by the terms of the Agreement.

Users will be provided with a copy of the signed *Municipal Information System and Network User Agreement*. With respect to staff and Members of Council, the original signed Agreement will be filed in the user's personnel file. With respect to other authorized organizations and individuals, the original signed Agreement will be filed with other documents pertaining to the organization or individual.

4.21 Users must at all times respect trademark and copyright infringement laws, software licensing, and property rights. This includes refraining from copying any software licensed to the Municipality.

4.22 The sharing of usernames and passwords obtained for access to municipal systems and network resources is strictly prohibited. Anyone who obtains a username and password must keep that password confidential.

4.23 Users of municipal Internet access shall identify themselves honestly, accurately, and completely when participating in electronic communication and other interactive Internet-based activities, e.g., social media.

4.24 When accessing their municipal email account from their personal phone or any other means outside municipal systems and the network, users must exercise care to ensure these devices are secured and password protected. If using a public device to access municipal email, users must clear the cache of the device after logging out.

Penalty

4.25 Failure to abide by this Policy or the *Municipal Information System and Network User Agreement* may result in progressive discipline up to and including, but not limited to, confiscation of municipal equipment, and/or legal action as appropriate to the situation.

4.26 Users are required to report any observed or suspected incidents of non-compliance to the immediate supervisor of the individual suspected of being in violation of this Policy or the *Municipal Information System and Network User Agreement*. Failure to do so constitutes equivalence to participation in the activity and therefore incurs the same disciplinary action associated with non-compliance.

5. Responsibilities

5.1 Council will:

5.1.1 Ensure the Municipality has a current and comprehensive policy for acceptable system and network usage; and

5.1.2 Review and amend this Policy as required.

5.2 The Chief Administrative Officer or designate will:

5.2.1 Implement and administer this Policy; and

5.2.2 Identify and propose revisions to this Policy in consultation with IT staff.

6. Amendments

Date	Amendments
August 2021	Transferred to new template and harmonized with User Agreement.

Schedule A

Municipal Information System and Network User Agreement

I acknowledge that I have received and read a copy of *Policy IT-07-001 Acceptable System & Network Use* of the Municipality of the County of Kings. I understand and agree to abide by the terms of this policy.

I realize that the Municipality of the County of Kings may record and store copies of electronic messages that I send and receive, the Internet address of any site that I visit, and all network activity of devices connected to the network. Municipal IT staff and management may review this information as necessary.

I understand that any deliberate violation of this policy may result in immediate disciplinary action, as described in *Policy HR-06-003 Employee Conduct* of the Municipality of the County of Kings, or in accordance with the Collective Agreement, whichever is applicable. Any action that may be subject to criminal prosecution will be referred to local law enforcement.

_____

Signature

_____

Name (Printed)

_____

Date