Title

1. This policy shall be known and may be cited as the **Technology Acceptable Use Policy**.

Scope

2. This policy applies to:
    a. Staff, Elected Officials, Contractors, Partners, and others using Technology in a Municipal Building, or working on behalf of the Municipality at any location, including home based or remote work.
    b. Use of Municipally owned laptop or desktop computers, cell phones, tablets, or other electronic devices.
    c. Use of Municipal building control systems, signage, video surveillance systems, printers, and industrial control (SCADA) systems.
    d. Use of Municipal data networks – including "guest" networks – provided by the Municipality by any device, including personally owned devices where such usage is authorized.

Rationale

3. The Municipality provides Technology for the purpose of providing Municipal services to its citizens. While other usage, including limited personal use as defined in this policy, may be acceptable, this policy is primarily concerned with the following:
    a. **Legal Compliance**;
    b. **Providing a Safe, Welcoming, and Inclusive Workplace;**
    c. **Clarifying and Reinforcing Expectations;**
    d. **Maintaining Technical Capabilities and Performance of Municipal Systems;**
    e. **Protection of Municipal Assets;**
    f. **Cyber Security; and**
    g. **Maintaining Organizational Reputation and Workplace Culture**

No Expectation of Privacy

4. Users of Municipal Technology or data networks should be aware that any activity may be monitored for performance, troubleshooting, and compliance purposes. **There should be no expectation of privacy while using Municipal technology.**

Policy

5. For the purposes of this policy, use of the word **AUTHORIZED** shall imply authorization by the Chief Administrative Officer.
6. **The following activities are prohibited** while using Municipal technology:
    a. **Illegal Activity –** any activity that is in violation of International Law, the Criminal Code of Canada, the Laws of Nova Scotia, or Municipal Bylaws.
    b. **FOIPOP / PIIDPA / MGA Violations –** this may include using Municipal Technology for any purpose that violates the legislation or jeopardizes another individual's personal privacy, as well as transporting a Municipal device or Municipal data (including electronic transmission) outside Canada without obtaining prior authorization.
    c. **Improper Storage of Municipal Data**
        i. Municipal data may only be stored in locations authorized by the Municipality (currently including but not limited to Microsoft OneDrive, Teams, SharePoint, Outlook, and Diamond).
        ii. Users may not use third-party cloud-based storage (such as DropBox, Google Drive, iCloud, Sync and others) for storing Municipal data. These services may be accessed if files are shared from an external organization (i.e. consultants, PNS, Government of Canada).
        iii. Unencrypted storage of data on USB or other external storage is prohibited.
    d. **Inappropriate Usage**
        i. Using Municipal technology to produce, send, receive, print, or otherwise access and disseminate material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, bullying, defamatory, racist, or other material that may be deemed to be undesirable by the Municipality.
        ii. Accessing file sharing sites or applications (BitTorrent, Android TV, and other similar services)
        iii. Gambling and online Gaming
        iv. Accessing online dating apps and services
    e. **Copyright or License Violations**
        i. Improper downloading of copyrighted material, including video, audio, and graphical content.
        ii. Use of images or other intellectual property in work products (websites, presentations, newsletters, etc.) without a valid license or authorization from the copyright holder.
        iii. Installation of software downloaded from any source without authorization.
    f. **Unauthorized Access –** other than for the purposes of approved generic accounts and workstations (i.e. Kiosks, reception computers, Council presentation equipment):
        i. Using or attempting to use another's computer or email account password without authorization.

ii. Allowing another person to use your computer or email account.
iii. Accessing data, documents, or records that are not required for the performance of your duties or enabling others to do so.
iv. Allowing a third party (family member, independent service technician, friend) to access, modify, or otherwise use your Municipal device.

g. **Theft or Destruction of Data –** including malicious modification or deletion of data, unauthorized bulk deletion of email records, and copying Municipal data without authority (including scanning or photographing Municipal documents).
h. **Tampering with Security Controls**
    i. Altering or otherwise interfering with security settings on Municipal Devices relating to automatic updates, antivirus, firewall, network, and remote management settings.
    ii. Installation of unauthorized remote access software (Chrome Remote Desktop, TeamViewer, AnyDesk, VNC, etc).
    iii. Installation or use of unapproved VPN software or configurations.
i. **Unauthorized Hardware Modifications –** excepting the attachment of approved peripherals (keyboards, mice, monitors, printers, etc):
    i. Addition to or removal of hardware components from Municipal devices without authority.
    ii. Any activity that may invalidate the manufacturer's warranty.
j. **Hacking –** the following activities are actively monitored and are prohibited:
    i. Attempting to access restricted portions of the data network, an operating system, or security software.
    ii. Using hacking tools including password crackers, Wi-Fi scanners, packet analyzers, keyloggers, and others.
    iii. Deliberately initiating activity that could be construed as a denial-of-service attempt either internally or externally.
    iv. Tampering with or otherwise altering data wiring and cabling without authorization.
k. **Personal Use of Industrial Control (SCADA) systems** – the personal use provisions of this policy do not apply to building control, signage, video surveillance, and Industrial Control (SCADA) systems. Personal use of these systems of any type is prohibited.
l. **Usage for Commercial or Political Business –** except as authorized for the conduct of Municipal Council business and allowed under the Nova Scotia Elections Act:
    i. Use of Municipal devices, accounts, or networks for commercial or personal advertisements, solicitations, promotions, "pyramid" or multi-level-marketing schemes, or other commercial activities not related to Municipal work.
    ii. Use of Municipal devices, networks, or accounts for political purposes promoting any candidate or political party.
m. **Excessive Personal Use** – any personal use that exceeds the duration or other limits specified under the "Allowable Personal Use" section of this policy, personal use that

interferes with the use of others in providing Municipal services, or personal use that incurs direct or indirect financial costs to the Municipality.

Reporting Violations

7. Users who are aware of or suspect violations of this policy are required to report them to their Supervisor, Chief Administrative Officer, or to Strait-IT (in that order of precedence).

8. Suspected violations of this policy will be investigated in accordance with Municipal Council / HR practices, applicable procurement policy, and/or collective agreements as applicable. Substantiated violations may result in administrative or disciplinary action as prescribed in the Municipal Human Resources Policy, restriction or termination of contracts, or actions as outlined in the Municipal Code of Conduct for Elected Officials.

9. All occurrences of illegal or suspected illegal activity will be promptly reported to the appropriate law enforcement agency.

Acceptable Personal Use

10. The Municipality provides Technology principally for the purpose of conducting Municipal Business. Recognizing the requirements for work / life balance, managing childcare, and other factors that impact our daily lives, the Municipality allows for ***incidental*** personal usage of Municipal Technology.

11. Personal usage should be limited to times that are appropriate for doing personal things, such as scheduled breaks and lunch hours, or such other times as approved by a supervisor.

12. Personal use outside of normal working hours or outside the office should comply with other aspects of this policy regarding personal use.

13. Users may use "public" wi-fi networks to connect personally owned cell phones, provided such usage does not negatively impact the provision of Municipal services.

14. All users should be aware of their environment when using Municipal technology for personal use. What may be appropriate in a meeting room or private office may not be in an open workspace or in the view of the public.

Equipment

15. All technology used in the conduct of Municipal business shall normally be owned and managed by the Municipality. Any exceptions to this guidance (contractors, auditors, and other circumstances) must be approved by the Chief Administrative Officer in consultation with Strait-IT. **Use of personal devices to conduct Municipal business is not normally permitted and, other than cell phones, should not be in the workplace.**

16. End users assigned equipment for Municipal use are expected to take reasonable precautions to prevent physical damage and shall report any such damage promptly. Users may be held responsible for costs related to repairs or replacement of damaged municipally issued equipment due to reckless or negligent actions.

17. Where product accommodation is required due to physical, sensory, or other impairment, the CAO and Strait-IT shall work with the user and other medical or subject-matter experts to ensure technology is accessible and appropriate.

18. Computer equipment which is no longer required shall be retained by the Municipality to ensure secure data disposal, redeployment within the Municipality, or other usage as approved by the Chief Administrative Officer.

19. No departing employee or elected official may retain any Municipal Technology when they leave the employment of the Municipality, unless such technology is of a personalized nature to address a physical, sensory or other impairment and cannot reasonably be reused by someone else. The Chief Administrative Officer shall authorize retention in such cases.

20. Users **may** be held responsible for costs related to repairs or replacement of damaged municipally issued equipment due to reckless or negligent actions.

21. Installing software that is not authorized for usage is prohibited.

Record of Changes	
Initial Draft	12 December 2024
Second Draft	9 January 2026
Policy Notice & Review: Policy Approved By Council:	February 3, 2026 February 17, 2026

Chief Administrative Officer

Feb 18, 2026
Date