Title: Information Technology Acceptable Use Policy	
Policy Group: Your Government and People	**Policy Administrator:** Information Technology
Resolution No. **CW-118-2022**	**Policy Number:** **IT-02**
Approval Date: **2022-05-12**	**Revision Date:** **2026-05-12**

1. Policy Statement

- Prince Edward County (The County) is committed to providing the most efficient, effective and secure technology environment to the users of its Technology Services.

- The Acceptable Use Policy identifies roles, responsibilities, and requirements for the appropriate use of technological services and equipment issued and owned by The County.

- Authorized users are granted permission to use data, systems, and technologies that belong to The County in accordance with this Acceptable Use Policy.

2. Purpose

- The purpose of this Policy is to outline the acceptable use of technological services and equipment issued and owned by The County. These rules are in place to protect the employee and the County. Inappropriate use exposes The County to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

- This policy applies to all authorized users including employees, members of Council, or any individual retained by The County.

- The use of Mobile Devices issued by the County shall be in accordance with Appendix A.

- Failure to conform to the requirement of this Policy may result in disciplinary action-up to and including termination, legal action, and/or possible criminal proceedings.

4. Legislative Authority

- The Policy is intended to support and augment the following policies and legislation, agreements binding The County dealing with related matters:
    - Code of Conduct for members of Council
    - Employee Code of Conduct
    - Records Retention By-law
    - Respect in the Workplace Policy
    - Purchasing By-law
    - Criminal Code of Canada
    - Municipal Freedom of Information and Privacy Act

5. Definitions

a) **Authorized user(s)** means a defined as an employee, student, intern, volunteer, councillor, Mayor or board member of The County or its agencies who uses Corporate issued or owned technology or devices.

b) "**Mobile Device**" means any cellular or tablet connected to a cellular network that performs many of the functions of a computer, typically having a touchscreen interface, internet access, and an operating system capable of running downloaded applications.

c) **Technology equipment (Hardware)** means a group or “family” of products, which include devices that have a primary function related to the collection, transfer, storage, or processing of electronic data, such as desktops, laptops, tablets, printers, wireless devices, printers, etc.

d) **Technology services** means specialized technology-oriented solutions that combine the processes and functions of software, hardware, networks, telecommunications and electronics and facilitate the use of technology by end users.

e) **Software** means a generic term used to describe computer programs Data – information processed and stored by a computer.

f) **Network** means a group of two or more computers linked together and the associated infrastructure to enable this functionality.

g) **Remote** access means the ability to access a computer from a remote location and that County information and data is adequately safeguarded.

6. General

- Users of electronic information sources such as the Internet are expected to use these resources in a responsible manner, consistent with the educational, informational and recreational purposes for which they are provided, and to follow the rules and regulations of the county providing these resources.

- The County will provide employees with the technology required to carry out their job roles. Each department is responsible for identifying their own technological needs and recommending access levels for staff members.

- The County believes that productivity and communications are greatly enhanced through the appropriate and effective use of the County's electronic services. These systems include, but are not limited to: corporate data, software licensing, Hardware, passwords, internet access, email, access to email, files and the Internet, productivity software, business applications and databases.

- Authorized users must:

    i. Corporate Data:
        a. Ensure the corporate data for which he/she is responsible is accurate and up-to-date.
        b. Ensure the data is not distributed, copies, or used for any other purposed other than business.
        c. Maintain compliant with Municipal Freedom of Information and Privacy Act
        d. Ensure data is stored in the appropriate assigned location in accordance with the County's Records Retention By-law.

    ii. Software Licensing/Copyright
        a. Not download, copy of install any software for which The County does not have a license agreement or for which approval from Information Technology was not obtained.
        b. Not download, copy, or install any electronic data files, e.g. music, movies, or ebooks, that violate copyright laws, or violate any existing software licensing agreements.

c. Coordinate with Information Technology to download, copy, or install approved software or electronic data files.

iii. Hardware
   a. Use Hardware for The County's business purposes.
   b. Not move Corporate Hardware that are designated to be stationary (e.g. PCs, desk Phones, printers) without consent from Information Technology.
   c. Ensure Hardware, including laptops, handhelds, smartphones, are protected and secure from theft, loss, or damage.
   d. Ensure Hardware is screen locked, i.e. password protected, when leaving the system unattended.
   e. Return all assigned Hardware to his/her supervisor upon termination of employment or when job duties no longer require use of the Hardware.
   f. Know that only Information Technology staff are authorized to alter, modify or dismantle Hardware.

iv. Passwords
   a. Keep passwords private and secure.
   b. Users are fully responsible for all activities invoked through their userID and password.
   c. Know that an assigned UserID and password does not constitute user privacy, but is for the purpose of user authentication and authorization and does not preclude The County access.
   d. Change passwords whenever they are suspected of no longer being private and secure.
   e. Use Information Technology’s password procedure for the resetting or assigning of new passwords.
   f. Ensure that the password complexity selected is at an acceptable security level.
   g. Assigned certificates should be treated as passwords and kept private and secure.

v. Internet Access
   a. Ensure proper usage of the Internet. Proper usage includes but is not limited to, the following networking with colleagues, vendors, industry professionals and professional associations; researching and sharing authorized information; conducting The County's business.

vi. Electronic Mail

a. Know that electronic mail messages are considered corporate data subject to *MFIPPA.*
b. Maintain the confidentiality of electronic mail messages with discretion or as applicable, except where disclosure is required by law.
c. Use electronic mail for the Corporation's business purposes.
d. Use the County e-mail account when conducting the County's business; this includes while working outside the workplace.

vii. Corporate Telephones and systems

a. Use County telephones and voicemails for conducting County business purposes.
b. Maintain the confidentiality of voice mail messages with discretion or as applicable except where disclosure is required by law.
c. Report unusual occurrences with his/her voice mail, such as frequent hang-ups, off work-hour activity, and suspicion of password tampering.
d. Know that telephone calls and voice mail messages may be monitored and subject to MFIPPA.

7. Responsibility and Implementation

- Council is responsible for approving this Policy and making changes to this Policy.

- The Chief Administrative Office is responsible for:
  - directing compliance and resolving any conflicts with this Policy; and
  - approving procedures.
  - Promptly authorizing expenditures for incident containment, response and investigation services.

- The Manager of Information Technology is responsible for:
  - The administration and management of practices in compliance with the principles set out in this Policy;
  - Communicating amendments to the Policy or its procedures to authorized users;
  - Report any infractions to their supervisor and track infractions;
  - When acquiring any technology, adhere to the County Purchasing By-law; and

- Reviewing this Policy, along with its associated principles and guidelines, every four years, or earlier if needed, in order to ensure continuing relevance and conformance with best practices.

- Information Technology Help Desk is responsible for providing internal and external support.

- All Directors, Managers, and Supervisors are responsible for:

  - Ensuring all staff have read and understand the training materials provided to them, including any updates.
  - Ensuring that staff are compliant with this policy.
  - Ensuring that any violations of this policy are addressed and that proper coaching and/or disciplinary actions are taken.

- All authorized users are responsible for:

  - Reading and understanding all training materials provided to them, including any updates.
  - Using the technology for business purposes that benefit The County and are directly applicable to their job.
  - Reporting any suspected infractions to their immediate supervisor.
  - Taking reasonable precautions to ensure the integrity of the technological devices and networks.

8. Documentation and Forms

- The following are associated procedures of this Policy:

  - IT-02-01 Acceptable Use Procedures
  - IT-02-03 Email Standard Acceptable Use Procedures
  - Appendix A - New Employee New User Access Change Request Form

Appendix A - Acceptable Use of Mobile Devices

1. The following sections govern the acquisition, usage and management of cellular telephones and electronic devices. In addition, it outlines standards and procedures for appropriate use of mobile devices.

2. A Mobile Device can be a useful and effective tool for effective and timely communications to meet the operational requirements of the Prince Edward County.

3. The County is committed to providing wireless communication devices, where needed, to improve the operations of the municipality where:

    - These communication devices have been identified as a necessity due to work and meeting schedules and associated travel requirements that frequently interfere with the ability to communicate in person or via regular telephone.

    - The increasing municipal responsibilities associated with emergency preparedness create the need for instant communication capabilities beyond the normal workday and workweek.

    - Departmental needs depending on the nature of the departmental services.

4. This applies to all County employees, Members of Council, and any other persons issued or using a device in the conduct of municipal business who has been given access to the County IT Networks or data through mobile technologies. The category of devices to which this Policy applies to cell phones, and wireless telecommunications devices such as tablets.

5. The protocol sets out broad principles and establishes expected standards of behavior when using Mobile Devices owned/issued by the County and/or accessing County Networks and data.

6. Recognizing that employees and Council access these resources (phones, Network, data in varying ways, including through the use of personal equipment; it is expected that these individuals will adhere to the provisions of this Policy as it relates to each type of usage, including but not limited to:
    - In accordance with the *Highway Traffic Act Section 78.1(1)* No person shall drive a motor vehicle on a highway while holding or using a hand-held wireless communication device or other prescribed device that is capable of receiving or transmitting telephone communications, electronic data, mail or text messages. Users in violation of this section shall be held personally responsible for any charges or damage that may occur.

- The primary function of any device owned and issued by the municipality shall be related to conducting the operations of The County.

- A County issued device may, from time to time, be used for personal calls, so long as this use is incidental to its primary business use. Al

- Managing their voice/text/data usage and ensuring they adhere to their Mobile Device plan.

- Mobile Devices may not be used to conduct illegal transactions, harassment, or any other unacceptable behavior.

7. All reasonable precautions should be taken to ensure the security of Mobile Devices, an individual issued a device shall immediately report a lost, stolen or damaged device to their manager.

8. Upon termination, change of duties or at the request of their manager, an individual who has been issued a device shall return that device to The County.

9. All users of municipally issued Mobile Devices are advised that records related to calls and texts made on municipally owned mobile devices are municipal information. As such, information related to telephone numbers, length of call, time and date of call or text, as well as any downloadable data recorded on the Mobile Device, such as digital images (pictures), text messages or phone book entries, are subject to, and may be obtained under the provisions of *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56.*

10. The director is responsible for requesting issuance of a Mobile Device.

11. Human Resources & Organizational Development Department is responsible for reviewing the Policy with staff and ensuring all persons have signed the Policy Mobile Device Agreement.

12. The Information Technology Department shall issue the Mobile Device and configure the device with the appropriate programs.

13. All persons who have been issued a Mobile Device shall:

- Read and understand all training materials provided to them, including any updates.
- Ensure they have followed the appropriate approval and request procedures when traveling out of the country with a Mobile Device (See Data Management and Roaming).

- Taking reasonable precautions to ensure devices are not lost, stolen or damaged.

14. The following are associated procedures of this protocol:

- IT-02-02 Mobile Device