POLICY No. (2024-02)

Corporate Mobile Device Usage Policy

Originating Department	Innovation & Technology Services		
SMT Approval:	2024-07-17		
Council in Committee:	N/A	**Recommendation #:**	
Council Approval:	N/A	**Resolution #:**	
Revision History:		Click here for revision history	

1. PURPOSE

The Innovation & Technology Services (ITS) division distributes, manages, and supports Corporate mobile devices, such as cellphones for Haldimand County corporate employees and related staff. This policy seeks to outline ITS' approach for distribution and security of these Corporate assets in addition to the types of acceptable use for Corporate users of mobile devices.

2. SCOPE

This policy has been developed as a component of the Corporate Information Security strategy to ensure cybersecurity is a critical component of Haldimand County's holistic approach to promoting healthy and safe communities and managing risk. This policy applies to all Members of Council, Members of all Boards and Committees, Volunteer Firefighters, and all Employees of Haldimand County including full-time, part-time, casual, unionized, non-unionized, and Library staff.

This policy applies to all Haldimand County information technology mobile devices.

This policy supersedes section C – Mobile Apps, and Appendix D – Addendum for Users of County Issued Mobile Devices in the *Information Technology Acceptable Usage-Policy No. 2001-08*

3. DEFINITIONS

3.1 "Mobile Devices" includes any tablet or cellular phone that can transmit data, either through cellular or through WiFi, regardless of whether the device contains a SIM card.

3.2 “PHIPA” means The Personal Health Information Protection Act.

3.3 “MFIPPA” means Municipal Freedom of Information and Protection of Privacy Act

3.4 “Mobile Device Management” is the use of administration software installed on mobile devices to allow centralized command, control, and security of a digital fleet of devices. Functionality in a Mobile Device Management (MDM) system typically includes management of mobile apps, security policies such as passwords and pins, geo-location of devices, and remote deletion and wiping of devices.

4. LEGISLATIVE AUTHORITY

This policy is in alignment with the recommendations put forth by the Canadian Centre for Cyber Security (the Cyber Centre) and the Government of Canada’s “*Government in a digital age*” initiatives.

This policy is in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 1.1

5. POLICY ADMINISTRATION

Mobile Device Ownership

Mobile devices are corporate-owned and allocated to positions, not individuals. ITS is responsible for the procurement, activation, management, and deactivation of all County mobile devices regardless of the funding source of the device. ITS will provide training, mobile device repairs, and management of voice and data contracts. New initiatives which include the use of a Corporate mobile device must include the initial capital costs of mobile devices and be approved by the relevant divisional / general manager. Two (2) year replacement costs for Corporate mobile devices will be included in the ITS capital replacement budgets. Month to month operating costs for usage of mobile devices are to be paid out of the relevant divisional / departmental budgets as directed to ITS.

Mobile Device Renewal

Mobile devices should be replaced every two years to ensure they support the latest software and security requirements. Changes to the device selection are only practical during the two-year device renewal process as outlined in the *Mobile Device Selection* section of this policy. Any device changes desired for an existing position outside of this two (2) year cycle must be approved by the divisional / departmental manager and paid for by the requesting Division.

Mobile Device Selection

To encourage user adoption, and leverage existing user technological familiarity, ITS is committed to providing a selection of corporately supported devices for corporate users.

In practice this means ITS will provide options amongst the largest mobile brands available to the County.

Detailed device listings are included in Appendix A of this policy and will be updated every two years to align with device renewal.

Mobile Device Security

Innovation and Technology Services will be responsible for setting appropriate standards and guidelines for securing all corporately owned mobile devices. These standards and guidelines will be reviewed and updated overtime and must be conformed to by all corporate-owned devices. Attempts to circumvent established standards and guidelines will be treated as a policy violation.

Mobile Devices Acceptable Usage

Corporate Use: As directed by the relevant divisional / departmental manager, in alignment with the Haldimand County Code of Conduct, and in service of the employees job expectations.

Personal Use: Limited personal use is allowed during non-working hours (e.g., lunch or break times). Personal data such as photos or contacts are the employee's responsibility, and ITS staff are not responsible for preserving or securing this information. Any personal information stored on a Corporate mobile device may be subject to relevant FOI search requests as directed by the County Clerk.

Roaming Use: Mobile devices usage outside of Canada requires pre-approval by the employees relevant divisional / departmental manager. Certain executive employees and members of council may be given pre-approval to roam under specific circumstances (ie. a County-wide emergency) at the discretion of the relevant manager / CAO. Monthly usage information will be distributed to divisional / departmental managers for monitoring of excessive costs. Unapproved costs are expected to be reimbursed back to Haldimand County at the discretion of the relevant manager.

6. POLICY COMMUNICATION

This policy will initially be communicated to all staff, via email, from their relevant manager. Future communications to new employees will be via the established Human Resources on-boarding processes.

This policy will be posted to the intranet and on the public website.

Upon adoption of this Policy all users, as defined in the policy Scope, out of compliance will be required to comply based on the tenets set out in this Policy.

Innovation & Technology Services will audit user compliance to this Policy and report breaches to the Information Technology Governance Committee.

7. Policy Enforcement & Compliance

Violations of this policy will be referred to senior management and may result in disciplinary action. Employees must adhere to all relevant legislation, including MFIPPA and PHIPA.

8. Reference

This policy should be read alongside the Information Technology Acceptable Usage Policy, applicable collective agreements or policies governing non-union employees, various health and safety policies and guidelines, relevant and applicable legislation, and any other policy that may become applicable and/or relevant.

Revision History			
Report	**CIC**	**Council**	**Details**
SMT ITS-2024	Date N/A	Date N/A	SMT Initial Approval – July 2024
	Date Rec#	Date Res#	
	Date Rec#	Date Res#	
	Date Rec#	Date Res#	

Appendix A – Device Options

Based on vendor availability, overall costing, and functionality ITS supports the following devices for corporate purchase and support.

SKU	Product Name	Internal Storage	Provider
IP15128BLK	Apple iPhone 15 128GB	128 GB	ROGERS
S24128BLK	Samsung Galaxy S24 128GB	128 GB	ROGERS