	TOWNSHIP OF SOUTH STORMONT
	Title: Mobile Device Usage Policy – Schedule "A" to By-law No. 2022-055
	Policy Department: Corporate Services
	Effective Date: July 13, 2022
	Revision Date:

1 POLICY STATEMENT

1.1 The Township of South Stormont provides Township employees and members of Council with access to necessary mobile device technology to effectively undertake their roles within framework that protects Township data and network security.

2 PURPOSE

2.1 The policy is intended to support municipal duties with mobile technology. This policy will also:

- enhance corporate data and network security;
- reduce and protect against possible legal and other exposures related to using the Township's Mobile Devices; and
- improve management and control of mobility costs.

3 SCOPE

3.1 The policy applies to all Township employees and members of Council who are authorized to have a Corporate-issued Mobile Device.

4 DEFINITIONS

4.1 "App" means an application, especially as downloaded by a user to a mobile device.

4.2 "Corporate-issued Mobile device" means a device owned by the Township and issued to eligible employees or members of Council for the purpose of conducting Township business.

4.3 "Mobile Device" includes Corporate tablets and laptops, Corporate-issued Mobile Devices.

4.4 "Mobile Device Management" (MDM) means a software system that enables the Township's Corporate Services department to manage Mobile Devices connected to the Township's network. Functionality includes provisioning, securing, monitoring and the ability to remotely wipe Corporate-issued Mobile Devices.

5 GENERAL

5.1 The Mobile Device Use Policy sets out broad principals and establishes expected standards of behavior when using Mobile Devices and mobile device access provided by the Township.

5.3 The Township, through the Records Management Program is committed to establishing and maintaining record keeping practices that meet its legislative, accountability and business obligations. Employees and members of Council are responsible for complying with the provisions of the Corporate Records Management Policy. For clarification, a record is information however recorded, in textual, numeric, graphic, video, audio or electronic, etc.

5.4 Employees eligible for a Corporate-issued Mobile Device must sign the necessary Acknowledgement Form, being Schedule "A" to this policy and meet the following criteria:

a) spend part of their time working away from their main workspace (office);
b) job duties are in public safety, requiring immediate or emergency response;
c) job duties support round the clock business infrastructure and systems;
d) job duties are required to respond promptly to urgent business-related email or communication needs; or
e) other reason — where a business case has been approved by the CAO

5.5 Approved employees or Members of Council, who have signed the necessary acknowledgement form, will be provided a Corporate-issued Mobile Device.

6 RESPONSIBILITY

6.1 Mayor and Council are responsible to:

a) Reinforce and support Mobile Device Usage Policy among members of Council.

6.2 The Chief Administrative Officer (CAO) is responsible to:

a) Ensure all Directors are aware of this policy and of subsequent revisions.

b) Ensure compliance with these procedures and executing any necessary disciplinary measures.

6.3 Department Directors are responsible to:

a) Ensure employees with Corporate-issued Mobile Devices are trained and aware of provisions of the Mobile Device Usage Polices and subsequent revisions.

6.4 Employees and members of Council are responsible to:

a) Read and understanding all training material provided to them, including updates as they are provided.
b) Ensure they have followed the appropriate approval and request procedures when travelling out of country with a Mobile Device.
c) Take reasonable precautions to ensure Mobile Devices are not lost, stolen or damaged.

6.5 The Corporate Services department is responsible to:

a) Provide accurate, timely and available training material to Mobile Device users.
b) Provide timely Mobile Device support via the Help Desk ticketing system.
c) Wipe and/or locking lost, stolen or otherwise compromised Mobile Devices that have been reported.
d) Coordinate the purchase of Mobile Devices, associated accessories and assisting with the activation of mobile plans on new Corporate-issued Mobile Devices.

7 SECURITY

7.1 All Mobile Devices will be licenced with the Township of South Stormont MDM system regardless of the intended use of the device.

7.2 All Mobile Devices that access the Township's network or are used to store Township data (including email), must be protected by using a password that meets the provisions of the Township's Password Policy.

7.3 Employees or members of Council will immediately notify Corporate Services and their respective Director if their Mobile Device is lost, stolen or is believed to have had its security compromised in any way.

7.4 The MDM software, including any apps it may install, must not be removed from the Mobile Device.

7.5 Employees and members of Council are strictly prohibited from "jail breaking", "rooting" or performing any other changes that disables or modifies the hardware and operating system restrictions inherent on Mobile Devices.

7.6 Users with Mobile Devices outfitted with fingerprint readers, facial recognition or other similar option may be permitted to register this feature. Management reserves the right to remove this element if it is proven to be an unacceptable security risk.

7.7 The CAO, with input from Corporate Services, reserves the right to disconnect any Mobile Device from the Township system.

7.8 Corporate Services, following consultation with the CAO, will wipe any Mobile Device that is lost, stolen or is found to be in non-compliance with this policy.

7.9 Unless otherwise approved by the CAO, all Mobile Devices must be returned to Corporate Services on termination / resignation / retirement, during periods of short / long term disability, during any other extended period of absence from work, or if requested to do so.

7.10 End of life Corporate-issued Mobile Devices will be wiped and destroyed as provided in the Township's Information Technology procedures.

8 SUPPORTED DEVICES

8.1 The Township's Corporate Services Department will maintain a list of sanctioned Corporate-issued Mobile Devices.

9 DATA MANAGEMENT AND ROAMING FOR CORPORATE-ISSUED MOBILE DEVICES

9.1 Corporate-issued Mobile Devices will be set up with the Township's standard voice, text and data plan. This plan may change without notice, as approved by the CAO.

9.2 Employees and members of Council who wish to travel outside of Canada with their Corporate-issued Mobile Device (roaming) must:

a) Obtain authorization, in writing, from the CAO at least 10 business days prior to the travel date.
b) Upon approval of the CAO, arrange a roaming package through the Finance Department, that is required for the travel location and timeframe.

10 SOFTWARE ON CORPORATE-ISSUED MOBILE DEVICES

10.1 Users may install Apps on their Corporate-issued Mobile Device without the intervention of Corporate Services, providing the following criteria are met:

a) The App is not known to cause an unacceptable security risk, as determined by Corporate Services.
b) The App does not cause degradation in the performance of the Mobile device, as determined by Corporate Services.
c) The App is installed from approved sources, i.e. Apple App store, Google Play store.

11 REIMBURSEMENT OF COSTS

11.1 At the discretion of the CAO and in conjunction with the Corporate Services and Finance departments, failure to properly monitor and manage voice, text and data usage may result in the employs or member of Council to be financially responsible for covering costs above the Township's standard Mobile Device plan costs.

11.2 Employees and members of Council may be personally responsible for replacing lost, stolen or damaged Corporate-issued Mobile Devices, if reasonable care was not exercised.

11.3 The Township reserves the right to collect the costs through standard invoicing and collection and/or payroll deductions for charges exceeding authorized use.

11.4 Reimbursement amounts are subject to change, pending reviews of corporate Mobile Device Plans.

12 CONFIDENTIALITY

12.1 The Township is legally required to abide with certain confidentiality requirements and access procedures relating to records in the Township's custody or under its control. The requirements and procedures are set out in the Municipal Freedom of Information and Protection of Privacy Act. The records to which the Act related include all material stored on Township and/or other maintained systems. Employees and members of Council shall take all reasonable precautions to ensure compliance with the Act.

12.2 Before disclosing sensitive, confidential or proprietary information to third parties, by any means, employees and members of Council must seek authorization from their Director or the CAO.

13 COMPLIANCE

13.1 Employees and members of Council must comply with the guidelines contained with the Mobile Device Usage Policy and acknowledge receipt and understanding of this policy by endorsement of the Policy Acknowledgement Statement.

13.2 Failure to comply with the Township's Mobile Device Policy may lead to legal, punitive or corrective action up to and including termination of employment and corrective prosecution.

14. CONTACT

For more information on this policy, contact:

Director of Corporate Services/Clerk
Township of South Stormont
P.O. Box 84, 2 Mille Roches Road
Long Sault, ON K0C 1P0
613-534-8889, Ext. 201

Employee / Member of Council Acknowledgement

I confirm that I have read and understand the Township of South Stormont Mobile Device Usage Policy.

I agree to comply with the terms of the Mobile Device Usage Policy.

I understand that if I violate the rules of this policy, I may face legal, punitive or corrective action.

NAME: _____

POSITION: _____

SIGNATURE: _____

DATE: _____