Subject: Mobile Device Governance	Category: Policy
Policy No.: COS-IT-004	M&C Report No.:
Effective Date:	Next Review Date: (3 years)
Area(s) this policy applies to: City of Saint John employees; excludes elected officials, as well as members of agencies, boards, and commissions that manage their own devices.	Office Responsible for review of this Policy: Information Technology Service
Related Instruments: • **COS-CC-001** Access Policy • **COS-CC-003** Information Management Policy • **COS-CC-004** Information Security Policy • **COS-ITS-001** Internet, Asset, and Electronic Mail Acceptable Use Policy • **COS-CC-010** Privacy Policy • **FAS-014** Travel Policy for Employees • Telephony Device Allocation Guideline (Appendix)	Policy Sponsor: Chief Information Officer (CIO)
	Document Pages: This document consists of 14 pages.

Revision History:

Common Clerk's Annotation for Official Record

I certify that the –Insert Title-Policy Statement was adopted by resolution of Common Council on Month-Day-Year.

I certify that the –Insert Title -Policy was approved by the City Manager on Month-day-Year

_____ _____

Common Clerk Date

Contact: Stephanie Rackley-Roach
Telephone: stephanie.rackley-roach@saintjohn.ca
Email: (506) 639-8083

TABLE OF CONTENTS

1. POLICY STATEMENT

The purpose of the Mobile Device Governance Policy (the "Policy") for the City of Saint John (the "City") is to define the governing of City-owned mobile devices, which access City corporate information systems.

The Policy supports the following corporate objectives:

- Support employees in their contribution to establish the City of Saint John as a service-based, results oriented, high performance, public service organization by providing mobile devices appropriate to operational needs;
- Support the customer service needs of the organization by ensuring employees have the means to receive and respond to citizen or corporate requests within established service levels;
- Provide for sound fiscal management of the organizational cost of mobile devices by the establishment of criteria to guide the deployment of mobile devices based on the operational requirements of a Service Area;
- Protect the integrity and confidentiality of City data by establishing guidelines for mobile device access to City corporate information systems and for secure mobile device data storage; and
- Support Corporate Records and Information Management policies and practices in the achievement of efficient and effective information management.

2. SCOPE

The Policy applies to the use of mobile devices (i.e., cellular phones, wireless data devices, and smart phones) owned by the City and used by employees of the City of Saint John. The Policy does not apply to City of Saint John elected officials, nor members of City of Saint John agencies, boards, and commissions that manage their own devices.

In addition to City-owned mobile devices, sections *6.4 – Security* and *6.5 – Monitoring Access* also apply to personal mobile devices used to access City corporate information systems.

The Policy does not apply to laptop computers.

3. LEGISLATION AND STANDARDS

The Policy is related to the following policy instruments of the City of Saint John:

a) **COS-CC-001** Access Policy
b) **COS-CC-003** Information Management Policy
c) **COS-CC-004** Information Security Policy
d) **COS-ITS-001** Internet, Asset, and Electronic Mail Acceptable Use Policy
e) **COS-CC-010** Privacy Policy
f) **FAS-014** Travel Policy for Employees

g) Telephony Device Allocation Guideline (Appendix)

4. ROLES AND RESPONSIBILITIES

I. EMPLOYEES

All employees who use a City-owned mobile device are expected to:

a) read, understand, and comply with the Policy and the employee's responsibilities outlined therein;
b) pay in full any expenses indicated in the Policy as being subject to reimbursement by the employee; and
c) cooperate with any investigation or data search requirements as required by City of Saint John management, local police, or RCMP;

II. MANAGERS

In addition to the roles and responsibilities identified for employees, managers must:

a) be knowledgeable in all aspects of the Policy;
b) review the Telephony Device Allocation Guideline to determine the appropriate device has been identified prior to authorizing a City-owned mobile device for an employee;
c) ensure employees have reviewed the Policy, as well as any associated SOPs, and that said review has been recorded on their profile in Safetyhub prior to authorizing a City-owned mobile device;
d) serve as a resource to employees on the Policy;
e) personally review, or assign an appropriate designate to review, the monthly billings for City-owned mobile devices they have authorized for their Service Area;
f) ensure any expenses indicated in the Policy as being subject to reimbursement by the employee are paid in full by the employee; and
g) take appropriate steps to investigate any possible violation of the Policy.

III. INFORMATION TECHNOLOGY SERVICE (IT)

In addition to the responsibilities related to monitoring, security, and mobile device management, IT must:

a) be knowledgeable in all aspects of the Policy;
b) ensure the necessary approval has been received from the appropriate manager prior to deploying a City-owned mobile device or adding additional services/travel plans to existing devices;
c) forward monthly billings for City-owned mobile devices to the appropriate managers and/or designates for review; and
d) inform the appropriate manager immediately should any violation of the Policy be detected or suspected.

5. MONITOR AND REVIEW

The Policy shall be reviewed every three (3) years by IT, or more frequently should changes in technology or other circumstances warrant.

6. IMPLEMENTATION

This policy shall be implemented by IT. All current users of City-owned mobile devices shall be required to review the Policy, as well as any associated SOPs, within three (3) months of the module becoming available in Safetyhub.

All future users of City-owned mobile devices shall be required to review the Policy, as well as any associated SOPs, prior to their manager authorizing deployment of a device.

6.1 ELIGIBILITY FOR MOBILE DEVICES

Provision of a City-owned mobile device is based on the operational requirements, safety considerations, and service level standards of a Service Area in order to facilitate City business or provide customer service. Mobile devices are issued to users for the express purpose of conducting City business.

The Service Area manager must approve all requests for City-owned mobile devices. In determining approval for a City-owned mobile device, managers should use the Telephony Device Allocation Guideline to determine how best to address the telecommunication needs of an employee.

IT will not provide an employee with a City-owned mobile device until IT receives approval directly from the appropriate manager.

To determine the type of mobile device to provide to an employee, a manager must weigh the cost of providing a cellular phone, smart phone, or wireless data device with regard to service needs. All mobile devices that will be accessing the City's corporate information systems must be selected from makes and models approved by IT, as there may be security implications. Any applicable chargeback fees for devices purchased by a department will continue to be charged to that department until the device is redeployed by IT.

Mobile devices issued by the City may be removed from a user at the discretion of the Service Area manager or the CIO at any time.

If a user goes on a period of extended leave of longer than one (1) month, the City-owned mobile device must be returned to IT. A City-owned mobile device may only be retained by an employee on extended leave if special permission is granted by the authorizing manager; the evaluation of the employee's circumstances will be left to the discretion of that manager.

6.2 MOBILE DEVICE PURPOSE

6.2.1 GENERAL USAGE

City-owned mobile devices are to be used for business purposes related to an employee's duties for the City.

An employee may make limited personal use of a City-owned mobile device to:

- communicate with friends and family;
- pursue independent learning that may not be directly related to the performance of one's employment responsibilities; and
- perform public service, such as non-employment related community and/or volunteer activities.

Limited personal use consists of use that does not interfere with the performance of an employee's duties and occurs on the employee's own time, outside of working hours.

Any additional costs incurred as a result of personal use must be reimbursed by the employee. Please note that if changes should occur in Canada Revenue Agency's tax rules pertaining to the personal use of a corporate mobile device, there is the potential for it to be considered a taxable benefit.

IT does not provide technical support for the personal use of a City-owned mobile device.

A user is not permitted to use call forwarding to redirect incoming calls for a City-issued phone number to a non-City-owned device.

There is zero tolerance for a City-owned mobile device to be used for any commercial undertaking that is unrelated to the user's role as an employee of the City of Saint John.

The use of mobile device features, which shall include but are not necessarily limited to, roaming, special messaging services, video streaming, GPS tracking, and video calling, will be governed by IT as a cost and security control measure; such features may have the potential to result in high data usage or may have other implications. A user must check with IT and their manager prior to using such features and the use must support operational needs.

A user is not permitted to install third party applications (e.g., social media apps, games, email apps) unless an operational requirement for the application has been determined by their manager and approval has been obtained from IT. IT will investigate the third party application prior to authorizing installation.

There is zero tolerance for the use of City-owned mobile devices for unlawful or criminal activity and such activity may result in disciplinary action in accordance with the City's established disciplinary policies and procedures.

6.2.2 TRAVEL

Travel outside of Canada may result in significant long distance charges and roaming fees. Users are not permitted to use City-owned mobile devices outside of Canada unless a specific travel plan for the use of a mobile device is arranged with IT prior to travel.

Managers must ensure there is an operational requirement for a travel plan and weigh the benefit of travelling with a mobile device against the cost of a travel plan. Managers must provide travel plan authorization to IT prior to a plan being added.

Any employee that uses a City-owned mobile device outside of Canada without arranging for a mobile device travel plan will be personally responsible for any costs incurred by usage of that device. Should a user wish to add a travel plan for personal use of a mobile device, approval must first be obtained from their manager and the user must reimburse the City for the full cost of that plan.

6.2.3 TETHERING

Tethering to provide access to the Internet for any device not owned by the City using a City-owned mobile device's wireless connection is not permitted. Should data overages result from tethering for personal use, the cost can be substantial and it will be the responsibility of the employee to reimburse the City for overage costs.

6.2.4 DATA AND STORAGE

Any photos, videos, or other data stored on a City-owned mobile device are subject to the Right to Information and Protection of Privacy Act. Text messages are also considered records. Personal data of any nature is not to be stored on a City-owned mobile device and IT will not be responsible for the back-up or security of such data.

6.2.5 TERMINATION OF EMPLOYMENT

Upon ending employment with the City of Saint John, the user must return all City-owned mobile devices (and any accompanying accessories) unlocked to IT, and provide any passwords necessary to access the devices; otherwise, the user will be billed for the replacement cost of the equipment.

6.3 MOBILE DEVICE MANAGEMENT (MDM)

IT uses mobile device management (MDM) to secure mobile devices and enforce policies remotely. Before connecting a mobile device to City corporate information systems (e.g., email, City of Saint John software), the device must be configured for access by IT.

MDM will only be installed by IT on City-owned mobile devices connecting to City corporate information systems.

MDM enables IT to take actions on mobile devices such as remote wiping, location tracking, application visibility, and hardware feature management.

Any attempt to contravene or bypass MDM will result in immediate disconnection from all City corporate information systems and may be subject to disciplinary action.

Users will not make any modifications to the hardware or software that change the nature of the device. This includes, but is not limited to, applications that avoid or circumvent IT-used MDM.

6.4 SECURITY

All mobile devices accessing City corporate information systems must be protected by a password and users are strictly prohibited from disclosing this password to anyone.

All users of City-owned mobile devices must employ reasonable physical security measures. Users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

If a City-owned mobile device and/or its accompanying accessories are lost, stolen, or damaged as a result of the user's negligence (as determined by the authorizing manager), the user will be required to reimburse the City for the replacement cost of the damaged goods and/or the fees related to the cancellation of the service for that device.

In the event of a lost or stolen mobile device, the user must immediately notify IT. IT will remotely wipe the mobile device of all data and lock the device to prevent access by anyone other than IT. The remote wipe will destroy all data on the device, whether it is related to City business or is personal in nature. If the City-owned device is recovered, it will be submitted to IT for re-provisioning.

Users are not permitted to backup City information using any non-City-owned computer, device, or remote data storage.

Any mobile device that is used to access City corporate information systems must adhere to the security protocols and password requirements of IT.

IT will manage security, network, application, and data access using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the City's established disciplinary policies and procedures.

6.5 MONITORING ACCESS

Monitoring is necessary in order to identify accounts or computers that may have been compromised by external parties or users who are not complying with City policies.

IT can establish audit trails for internal review, which may be accessed and used without notice. Such audit trails will be able to track access of mobile devices to City corporate information systems and the resulting reports may be used for investigation of possible breaches and/or misuse. Users agree to and accept that this access and/or connection to City corporate information systems may be monitored to

record dates, times, and duration of access in order to identify unusual usage patterns or other suspicious activity.

6.6 MONITORING USAGE

The City may monitor any use of City-owned mobile devices and any access to City corporate information systems. If the City discovers activities or has reason to suspect activities that do not comply with the policies, business practices, or administrative procedures of the City, disciplinary action may be taken in accordance with the City's established disciplinary policies and procedures. Should activities of a criminal nature or activities that may otherwise violate the law be discovered, the City may notify the appropriate authorities.

Webmail and ActiveSync are the only methods approved by IT for accessing corporate email using a personal mobile device.

All users must ensure they are using a secure network when using a mobile device to connect to City corporate information systems and data.

7. AUTHORIZATION

The Mobile Device Governance Policy Document is authorized under the authority of the City Manager, on the recommendation of the CIO.

8. RESOURCES

Resources reviewed for the development of the Policy included the City of Fredericton's 'Wireless Usage Guidelines', the City of Moncton's 'Mobile Device Policy', the Town of Quispamsis' 'Hand Held Operated Electronic (Mobile) Devices Policy', and the Saint John Police Force's 'Mobile Device Usage Operational Policy', as well as policy documentation drafted in 2012 by previous City of Saint John staff.

9. PROCEDURES

Standard operating procedures for the implementation of the Mobile Device Governance Policy shall be developed as appropriate.

10. GLOSSARY

a) **ActiveSync**: a mobile data synchronization app that synchronizes data with handheld devices and desktop computers/servers.

b) **Cellular Network:** a radio network distributed over land areas called cells that when joined together by cell site transceivers provide radio coverage over a geographic area.

c) **Corporate Information Systems:** the various software and tracking systems used to conduct the business of a company or organization (e.g., email applications, payroll systems, databases).

d) **Internet:** a global computer network that provides a variety of information and communication facilities that consists of interconnected networks and uses standardized communication protocols.

e) **Mobile Devices**: for the purpose of the Policy, the term Mobile Devices refers generally to the following types of devices:

   i. Cellular Phone – a portable phone that is used to communicate over a wireless network, including smart phones.

   ii. Wireless Data Device – a device provisioned to use a cellular network to send and receive data. The device does not provide phone voice services. Wireless data devices include, but are not limited to: tablets, wireless internet devices such as internet sticks or air cards, or other peripheral devices that can connect to a computer to enable a computer to send and receive data using a cellular network.

   iii. Smart Phone – a portable device that combines both cellular phone and wireless data device capabilities, has an operating system that allows the device to run applications, and has internet capabilities.

f) **Personal Mobile Devices:** mobile devices owned by the device user and not by the City of Saint John.

g) **Right to Information (RTI):** refers to the Right to Information and Protection of Privacy Act, S.N.B. 2009, c.R-10.6.

h) **Safetyhub:** the City of Saint John's online training system for employees.

i) **Tether:** the use of a smart phone as a modem to provide a laptop, or other data device, with access to the Internet using the phone's wireless data connection. This includes enabling the Personal Hotspot of a smart phone.

j) **Third-Party Applications:** a software program that is developed by a company other than the manufacturer of the mobile device operating system (e.g., social media apps, games, email apps).

k) **User:** any employee of the City of Saint John who uses a City-owned mobile device; this excludes elected officials, as well as members of agencies, boards, and commissions.

l) **Webmail:** any email client (e.g., Microsoft Outlook) implemented as a web application running on a web server.

m) **Wireless:** for the purpose of the Policy, the term wireless refers to data and/or voice services provided over a cellular network.

11. INQUIRIES

Inquiries about the Mobile Device Governance Policy may be directed to the Chief Information Officer.

12. APPENDIX

Telephony Device Allocation Guideline.

Telephony Device Allocation Guideline

Responsible Executive: Commissioner of Finance
Responsible Office: Information Technology
Date Issued: July, 2016
Date Last Revised: July, 2016

TABLE OF CONTENTS

CONTACTS

Subject	Contact	Telephone	Email/Web Address
Guideline Clarification	Commissioner of Finance	658-2951	
Daily Management	Telecommunications Specialist	649-6047	servicedesk@saintjohn.ca

STATEMENT OF GUIDELINE

This guideline directs managers and staff in how to determine which telephony device should be allocated and aides in the establishment of expectations of use as per the role of the user. It promotes a best practice and impacted parties are clear on their role and responsibilities. This guideline is to be read prior to making hardware sections on the IT Access Form.

REASON FOR THIS GUIDELINE

As part of continuous improvement efforts, it was determine that many staff are allocated two telephony devices (land and cellular) when in many cases one becomes underutilized and they can perform their role with one device. It was also determined that in many cases, expectations of use where not clearly conveyed to staff. Additionally, a new mobility contract provides for some unlimited uses that make it feasible to use one device only.

INDIVIDUALS AND AREAS AFFECTED BY THIS GUIDELINE

All service areas requesting/authorizing a telephony device are subject to this guideline.

EXCLUSIONS

None

RESPONSIBILITIES

Commissioner of Finance
Executive authority supporting adherence to the guideline and ensures the proper resources are in place to execute and uphold this guideline.

Manager of Information Technology
Supports Telecommunications Specialist in daily management of guideline and acts as escalation point for deviations.

Telecommunications Specialist
Coordinates the telecommunications functions specific to this guideline and ensures that the guideline is communicated, understood and followed on a daily basis. Measures adherence and reports deviations to Manager of Information Technology.

Managers
Reads and understands guideline and makes telephony device allocation decisions based on the best practices identified within the guideline.

Users
Reads and understands the guideline and follows best practices as outlined within the guideline.

BEST PRACTICES

Preamble

When possible, only one telephony device should be allocated to staff. When staff receives two devices, one may become underutilized and contributing to costly wastes. However, customer service should not be impacted and considering the City is diverse in services and roles one size does not fit all.

Considerations for land line use

- Generally works normal day shift hours.
- May attend meetings but generally in the office.

- Not in an emergency or 24/7 position/service.
- May or may not be customer facing.
- May or may/not have direct reports
- Can reasonably be away from office and manage contact through good practices of checking voicemails and keeping office attendants up to date.
- Uses computer for most of communication, email/Lync/Skype.
- May be on call but has access to an on call cell.

Considerations for cell use

- Works different shifts, a cell may be needed for safety reasons
- Very mobile, works in the field (safety and contact to office important)
- In an emergency 24/7 position/service.
- Customer facing (in the field).
- May or may not have direct reports but may coordinate vendors/contractors.
- Out of office frequently, needs to be accessible to direct reports.
- On call, no access to on call cell.

Consideration for both devices (which should be limited)

- Anticipated high frequency of use for both devices (benchmarked against existing similar roles)
- Lack of defined customer service.
- Cell used primarily for other uses than voice.
- High voicemail instances.
- Frequent lengthy voice situations.
- Emergency or security reasons.

RELATED DOCUMENTS, FORMS AND TOOLS

- IT Access Form

WEBSITE ADDRESS FOR THIS GUIDELINE

HISTORY AND UPDATES

APPENDIX

There are none at this time.