Category: ITS Policy Policy No.: ITS-02-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 7 Effective Date: Feb 7, 2024 Report No.: CPS-06-2024

Cellphone and Mobile Device Policy

Purpose

The purpose of the Cellphone and Mobile Device Policy is to:

- provide direction, terms, conditions and procedures for department directors and staff who use a Corporate Issued Mobile Device or a Personally Owned Mobile Device for the purposes of conducting Middlesex Centre business, and to;

- ensure the protection of personal information, confidential information and any other information in the custody and control of Middlesex Centre while being transmitted and/or stored on mobile devices.

Scope

This policy applies to all Authorized Persons who may conduct Middlesex Centre business using a Mobile Device.

Definitions

For the purpose of this document, the following terms have the following meanings:

"(ITS) Asset" means any physical electronic device owned by Middlesex Centre, which may contain or have access to sensitive information such as files and emails or has considerable value and is uniquely identifiable via a serial number or other means.

"Authorized Person(s)" means any employee, consultant or contractor of Middlesex Centre who has been approved by their respective department director to use a Mobile Device for business purposes.

"Corporate Information" is any and all information in the control and custody of Middlesex Centre.

"Corporate Issued Mobile Device(s)" are any Mobile Devices which are owned and issued by Middlesex Centre for use by the Authorized Person for business purposes.

"Information Systems" means any hardware or software system that people and organizations use to collect, filter, process, create and distribute data.

"ITS" means Information Technology Services.

"Mobile Device(s)" includes any cellphone, tablet, personal digital assistant or any other related mobile device that can access the Internet. For the purpose of this policy, laptops are not considered mobile devices.

"Mobile Device Management (MDM)" is a means of deploying, securing, monitoring, integrating and managing Mobile Devices. The intent of MDM is to optimize the functionality and security of mobile devices within the organization, while simultaneously protecting the corporate network and end-user.

"Monitoring Tool" is an application installed on a workstation, server, mobile device, or laptop which collects or logs information for the purposes of troubleshooting, data protection, or monitoring as defined under the Electronic Monitoring Policy.

"Personally Owned Mobile Device(s)" are any Mobile Devices which are owned and maintained by the Authorized Person and used for business purposes. The devices must adhere to the Mobile Device Security and Hardware Standards outlined later in this document.

Roles & Responsibilities

To ensure consistency and fairness, the management and connectivity of all corporate cellular accounts and Mobile Devices are the responsibility of the **Corporate Services Department** in collaboration with the Information Technology Services department at the County of Middlesex.

Department directors in consultation with the Director of Corporate Services may choose to assign a Corporate Issued Mobile Device to an Authorized Person or allow the Authorized Person to use their Personally Owned Mobile Device to conduct Middlesex Centre business. Among many other considerations, department directors must consider the sensitivity of the information which may reside on the Authorized Person's Personally Owned Mobile Device when making their decision. For example, if the Authorized Person accesses human resources information, the department director may choose to assign a Corporate Issued Mobile Device to ensure additional control over the information that may reside on the Mobile Device.

Persons who are authorized by their department director may use a Corporate Issued Mobile Device or may request to use their Personally Owned Mobile Device to conduct Middlesex Centre business while adhering to the terms, conditions and procedures outlined within this policy and any other applicable Middlesex Centre policies or legislation.

Middlesex County ITS shall take reasonable steps to ensure the safety and integrity of data stored on any mobile device capable of accessing corporate information as described in the Terms, Conditions and Procedures section of this policy.

Terms, Conditions and Procedures

1. Corporate Issued Mobile Devices

Staff may be provided with a mobile device such as a cellphone or tablet for the purpose of performing the duties of their job while employed at Middlesex Centre. Such devices shall be subject to the following provisions:

a) Mobile Devices shall be capable of performing the duty or task for which they were provisioned.

b) Staff shall not use any Mobile Device while driving or operating equipment and machinery, save and except for features operated by “hands free” technology.

c) From time-to-time, staff may utilize a Corporate Issued Mobile Device for personal use provided it does not impact the integrity or security of any corporate data or information stored on the device or exceed what could be considered reasonable use. Personal use must be in compliance with this policy and with the Acceptable Use of Technology Policy. Staff may not use a Corporate Issued Mobile Device to conduct business other than business related to the Municipality.

d) Staff shall take reasonable measures to ensure the device is kept in reasonable working order, except for normal wear and tear expected through the continued use of the device.

e) Mobile Devices shall be no more than four (4) generations old, and still receive regular security updates and support from the device manufacturer or vendor.

f) If issued a corporate mobile device, staff shall be responsible for ensuring the Mobile Device is kept up to date with current operating system patches and updates.

g) When updating a mobile device, the Department Director in collaboration with the Director of Corporate Services will complete a cost benefit analysis with respect to the current options by the Municipality’s mobile device provider.

h) Should a Corporate Issued Mobile Device become damaged through willful negligence, staff may be responsible for repairs or replacement of the device at the discretion of their department director and the Director of Corporate Services.

i) Staff shall be responsible for the reasonable safekeeping of Mobile Devices while in their care.

j) Staff shall take reasonable measures to ensure the device and any data stored on the device remains secure, such as not permitting unauthorized individuals to use the device, or leaving the device where it may be accessed by unauthorized individuals.

k) Staff shall inform their department director or manager should the device become lost, stolen, damaged or compromised.

l) Staff shall not attempt to alter any security controls or provisions, such as “jailbreaking” the Mobile Device.

m) Staff are encouraged to use physical protections such as screen protectors and are required to use cases for Mobile Device. These protections can be procured through Middlesex County ITS with approval of the staff member’s department director.

n) Mobile Devices shall be returned to Middlesex Centre’s Corporate Services Department and/or Middlesex County ITS at the completion of employment or during a scheduled Mobile Device upgrade. Some mobile devices are kept for use as spare devices in case of an emergency breakage. Exceptions to this provision may be granted at the discretion of the CAO and the Director of Corporate Services.

1.1 Cellular Roaming Packages for Corporate Issued Mobile Devices

Authorized Persons who require access to cellular services while roaming for work reasons (e.g., attending a conference in the United States, or required to stay in touch with their department/team while on a personal trip) must receive approval from their department director. The department director shall notify the Director of Corporate Services of this approval.

Authorized Persons who require access to cellular services while roaming for personal reasons, (e.g., for vacation) must receive approval from their department director. The department director shall notify the Director of Corporate Services of this approval and the employee will be required to reimburse the Municipality.

2. Personally Owned Mobile Devices

Authorized Persons who use their Personally Owned Mobile Device to access Corporate Information must adhere to the following terms and conditions:

a) Approval of department director and Director of Corporate Services shall be obtained before use.

b) Staff shall not use any Mobile Device while driving or operating equipment and machinery, save and except for features operated by “hands free” technology.

c) Mobile Devices shall be capable of performing the intended duty or task. Should a Personal Device not be capable of performing the intended duty or task, Middlesex Centre may recommend a Corporate Issued Device in-lieu of a Personally Owned Mobile Device.

d) Personally Owned Mobile Device shall be no more than four (4) generations old, and still receive regular security updates and support from the device manufacturer or vendor.

e) Staff shall be responsible for ensuring the Personally Owned Mobile Device is kept up to date with current operating system patches and updates.

f) Staff are responsible for any damage and normal wear-and-tear that may be caused to their Personally Owned Mobile Device.

g) Staff are responsible for any recurring service plans, warranty or maintenance fees, and any over-usage fees for the device, there will be no pre-arranged reimbursement agreements for the usage of the device.

h) Staff shall take reasonable measures to ensure the device and any corporate data stored on the Personally Owned Mobile Device remains secure, such as not leaving the device where it may be accessed by unauthorized individuals.

i) Staff shall inform their department director or manager should the device become lost, stolen, or compromised.

j) Staff shall not attempt to alter any security controls of provisions, such as “jailbreaking” their Personally Owned Mobile Device.

k) Staff are encouraged to use physical protection such as screen protectors and/or cases for their Personally Owned Mobile Device. Staff are responsible for any costs associated with procurement of these protections.

l) Middlesex County ITS shall remove access to any Corporate Data upon completion of employment or during Mobile Device upgrades.

m) Any cost associated with acquiring and maintaining a Personally Owned Mobile Device, including any charges or monthly fees incurred while using the device, is the sole responsibility of the Authorized Person.

3. Mobile Device Security and Hardware Standards

All Authorized Persons who are using either a Corporate Issued Mobile Device or Personally Owned Mobile Device to access Corporate Information must adhere to the following.

3.1 Access Control

ITS reserves the right to connect or disconnect any Mobile Device to or from Middlesex Centre’s Information Systems. ITS will engage in such action if such equipment is being used in a way that puts Middlesex Centre’s Information Systems, data, or users at risk.

All Mobile Devices attempting to connect to Middlesex Centre’s network through the Internet will be inspected using technology centrally managed by the ITS department. Mobile Devices that are not approved by ITS, are not in compliance with ITS security policies, or represent any threat to Middlesex Centre’s Information Systems, data or users will not be allowed to connect.

3.2 Mobile Device Management (MDM)

The ITS department uses Mobile Device Management software to secure Mobile Devices and enforce policies remotely.

All approved mobile devices configured to access corporate data, including corporate files and email, shall have Middlesex County approved Mobile Device Management software installed by

Middlesex County ITS. This policy includes Personally Owned Mobile Devices supported under this policy.

Employees accept that Middlesex County corporate information and/or data stored on the mobile device can be removed by Middlesex County ITS on behalf of Middlesex Centre, if:

a) the device is lost, stolen, or compromised

b) the device is not compliant with Middlesex Centre's policies

c) the device belongs to a person who is no longer working for Middlesex Centre

d) staff try to uninstall the Mobile Device Management Software from the Device

e) the device is rooted, jailbroken, or modified in any manner

Any attempt to contravene or bypass the MDM implementation will result in immediate disconnection from all Middlesex Centre resources, and there may be additional consequences in accordance with Middlesex Centre's policies.

4. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Any electronic records created using Mobile Devices as it relates to this policy, including but not limited to individual calls, e-mails, text messages and internet access is information that could be released to the public under MFIPPA. For clarity, this means any electronic records created using Corporate Issued Mobile Devices or Personally Owned Mobile Devices are captured under MFIPPA.

5. Electronic Monitoring

Any information on a Mobile Device which is accessible by the Mobile Device Management software may be subject to monitoring as defined in Middlesex Centre's Electronic Monitoring policy.

6. Termination of Employment

If an Authorized Person leaves the employ of Middlesex Centre, the Authorized Person must submit any and all Corporate Issued Mobile Devices to the Corporate Services department.

If the Authorized Person is using their Personally Owned Mobile Device to access Corporate Information, the device must be submitted to the ITS department to ensure all Corporate Information is appropriately removed from the personal device. If the device is not provided to the ITS department within a week, the device will be wiped remotely to ensure all Corporate Information is removed. This could cause loss of personal information that may be stored on the device, for which Middlesex Centre will not be responsible.

7. Compliance

Corporate Services and Middlesex County ITS enforce this policy and related standards. Anyone who has reason to suspect a deliberate and / or significant violation of this policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS and Director of Corporate Services.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.