CONESTOGA
Connect Life and Learning

WIRELESS AND MOBILE DEVICE TECHNOLOGY MANAGEMENT PROCEDURE

Authorizer: Senior Vice President, Academic / Student Affairs, Human Resources, Research and IT

Version: 1.0v

Effective Date: 8/18/2023

PROCEDURE STATEMENT:
This procedure outlines the College's position on the allocation and control of wireless and mobile devices, management of usage/data plans and the acceptable use of the College-owned asset. The use of Conestoga's corporate wireless and mobile devices and mobile plans is a privilege extended to authorized employees to support academic and administrative services. All users of Conestoga's wireless and mobile devices and plans must respect the rights of other users, the integrity of the physical asset and comply with all pertinent licenses and contractual agreements, as well as applicable provincial and federal laws, regulations, and College policies and procedures. Conestoga's wireless and cellular devices remain the sole property of Conestoga.

SCOPE:
This policy applies to all employees using corporate wireless and mobile devices.

DEFINITIONS:
"Mobile Device" is general term for any electronic device that can connect to a cellular network using the mobile service provider's SIM card installed within it.

"Wireless Device" refers to any kind of communication equipment that does not require a physical wire to relay information from one device to another.

"Enterprise Applications" are applications that serve centralized business functions to the College and are not installed locally on end user computer devices.

”Employee/User“ includes someone who has an active work agreement for Conestoga College and has access to a college paid wireless plan and device and/or technology asset.

RESPONSIBILITIES:

IT&S (Information Technology and Systems) Asset Management

Administrate the program of mobile devices at Conestoga and provide support in processes that enable mobile device usage at the College.

IT&S Service Delivery

Provide support, distribution, and reclaimant services for mobile devices.

IT&S Cyber Security and Endpoint Operations

Ensure mobile device compliance & data integrity.

Management Responsible for Device Users

Ensure that only users that require devices are issued devices to support their job duties and reclaim any devices if they are no longer required.

Employee/User

Adhere to all applicable policies and procedures in regard to wireless and mobile devices.

PROCEDURE ELABORATION:

General

The use of wireless or mobile devices paid by the College will be allowed under the following consideration(s):

- The job function of the employee requires them to be physically outside of normal office or work settings, and it is important to the College that the employee is accessible from these areas; and/or,
- The job function of the employee requires access to a voice network; in locations where internal voice services are not available (e.g., travel between campuses); and/or,
- The job function of the employee requires them to be accessible outside of scheduled or normal working hours.

The departmental Manager is responsible for determining that the purchase of College wireless or mobile device is warranted based on the criteria above. The requirement of the wireless or mobile device must be indicated on the request for position (RFP) when submitted to Human Resources (HR) and verified and approved by a Director/Chair when the employee applies for a device.

Hardware Procurement/Upgrade

With the corporate contract agreement, hardware is eligible for replacement after 2 years, however, unless the device no longer meets the requirements of the work, the employee

should not replace their device unless required. Issues that would require replacement include severe decreased battery life, physical damage making the device inoperable, screen size is not sufficient for role, etc. Replacing a device without a valid reason is not encouraged as it incurs unnecessary costs and is not in line with the college's strategic plan of sustainability (e-waste). Criteria for upgrading a mobile device outside of the 2-year contract will be allowed under the following conditions and subject to the departmental Manager's approval.

- Damaged phone where repair is more costly than upgrade.

Employees who require mobile devices to support their business function must acquire College-owned equipment through Conestoga's third-party portal. The third-party vendor requires the submission to be processed through a workflow which allows the employees' Manager and IT&S approval before being assigned.

Hardware Accessories
Required protective case/screen for all mobile devices are provided by the College and available when selecting a device. Different cases may be purchased at employee's expense with no re-imbursement. The employee is responsible for the device if it has been damaged due to non-use of a case.

Requests for accessibility accessories should be forwarded to HR.
All other accessories will be purchased by user without re-imbursement.

Software and Applications
Unless deemed necessary by job requirements, software and applications should not be loaded on College devices, including but not limited to social media, games, cracked or illegal software. The operating system of the device should not be rooted, broken, or otherwise modified from the standard deployment provided by the vendor.

The operating system and all applications should always be kept updated to a stable secured version.

Social Media
Use of personal social media on downloaded applications is not permitted on College-owned devices.
If you are required to use social media on behalf of the College and as part of your role, it must be managed through the college's social media management platform.

Porting Phone Numbers/Transfer of Liability
Porting a personal phone number to Conestoga College's corporate plan is not an option. Once an employee has left the college, they will not be permitted to port their number out.

Additional Features Required
In the event an employee(s) requires additional features beyond the standard mobility contract services to support business function(s), they will require departmental Manager approval and will need to contact IT&S to complete the changes in the system.

Monthly Charges Assessment
All equipment and services are invoiced to Conestoga College and processed by the IT&S department. Monthly, IT&S monitors individual usage and any additional costs incurred are scrutinized. If monthly charges exceed the set corporate plan, IT&S will be contacting the user for information and details on the charges. If there are any charges for excessive personal usage, they are to be reimbursed to the College by way of personal payroll deduction.

Leave Usage
Employees may be entitled to continue to use College-owned mobile devices during extended leaves (more than 6 months) or absences from the College, subject to the approval of their department Director or Chair. For those who will be out of country, please refer to the out of country usage section below.

In some cases, the department Manager may request mobile devices be returned when the absence is considered long, exceeding 6 months or more, and the Manager would like to temporarily re-distribute the mobile device to another employee, as warranted by the employee's business function(s). If the employee's position is being replaced by another individual, that device must be returned and provided to the new employee.

Stolen Property Procedure (Notification within 24 Hours)
Should a mobile device be lost or stolen, the responsible employee must immediately report loss by contacting the IT Service Desk- itsdesk@conestogac.on.ca – this is for the purpose of potential replacement, insurance claim, and / or filing a police report if applicable and depending on the circumstance.

Safe Keeping of Wireless and Mobile Devices
Employees with mobile device privileges must use and care for the devices in their possession in a responsible manner. Breakage, damage, or loss of equipment may lead to the need for reimbursement to the College of any associated costs incurred to the College, in relation to the repairs or replacement of the affected equipment.

Employees with mobile device privileges are required to keep devices clean, and in serviceable condition to the best of their ability. Mobile devices must have a protective cover, and when not in use, be placed in a secure location (e.g., locked desk or work bag).

Employees must keep batteries charged and report all irregularities immediately to the IT Service Desk.

There are several built-in protection mechanisms employees should be aware of in the day-to-day use of their mobile device. They include:

- Activate the “Keypad Lock” and PIN code (Check your user manual)
- For extended periods, (i.e., vacation days, etc.) switch the device off when not in use.

Mobile Device Management (MDM)
MDM will be administered on all College-owned devices. MDM allows IT&S administrators to control, secure and enforce policies on mobile devices. All data is College-owned and must be treated with respect and protected appropriately.

Home Usage
Secure the mobile device at home, as if it is your personal possession. Use the keypad lock, as you may be responsible for the unauthorized call charges billed to the mobile device if used without your knowledge or consent.

In Vehicle Usage
Mobile devices are not to be left in vehicles while unattended. These costs, while not necessarily claimable under insurance, may be charged back to the employee.
The use of mobile devices whilst driving is forbidden unless hands free function is activated. It is an offence (according to Section 78 of the Highway Traffic Act; Distracted Driving) to use mobile devices whilst operating a motor vehicle and the incursion of expiations and fines will be solely at the employee's cost. Any damage incurred because of this practice, which is not recoverable through insurance, may be charged to the employee.

Office Usage
While in the office, store the device and associated equipment with due care. Alternatively, the College’s unified communication system can be utilized on any technology device through the locally available wi-fi.

We encourage employees to utilize the systems and tools provided to them for communication.

Out of Country Usage
Any out of country usage must be reported to IT&S. An out of country access form is available through the IT&S website and must be submitted and approved by the employees Manager and HR before access is granted. Out of Country Access Form

Security – PIN numbers
PIN numbers are applied to mobile devices. Please ensure this feature is always used to minimize security risks as discussed elsewhere in this policy.

Do not share/disclose PIN with any other person.

Temporary Assignments
For temporary assignments greater than one month, where the position being filled is deemed to require a device, contact the IT Service Desk- itsdesk@conestogac.on.ca as options are available.

Offboarding
Devices that are no longer required must be returned to the IT Service Desk as soon as possible. This includes employees whose job has changed, and their new role no longer requires a mobile device. These devices are the property of Conestoga College and are a College tracked technology asset.

Violations
Violations of this Policy will be handled according to the specific violation's nature and severity. An employee who violates the Technology Lifecycle Management Policy and associated Procedures will be subject to disciplinary action. As a result, the College reserves the right to revoke use of a mobile device or technology asset at any time.

REFERENCES:
Technology Lifecycle Management Policy

Technology Asset Management Procedure

REVISION LOG:
8/18/2023 Academic Coordinating Committee