

NIPISSING UNIVERSITY

Policy Category:	General
Policy Number:	1.4.2018U
Policy Name:	Mobile Device Policy
Responsible Department:	Vice-President, Finance & Administration
Approval Date:	July 2018
Approval Authority:	Vice-President, Finance & Administration
Last Updated:	July 2018
Review Date:	July 2021

Definitions:

A mobile device includes, but is not limited to, cellular phones, smart phones (i.e. iPhone), tablet devices (i.e. iPad) and USB wireless modems.

Departmental authority includes person(s) who have signing authority within a unit under the Approval Authority Policy, 2.2.2012.B.

UTS is defined as University Technology Services.

1. MOBILE DEVICE POLICY

Purpose

- 1.1** This policy is designed to:
- Define employee eligibility for a mobile device;
 - Define the process for obtaining a mobile device and device upgrades; and
 - Provide guidelines on appropriate use, acceptable expenditures, and cost reimbursements.

Policy Statement

- 1.2** Device Eligibility
- Mobile devices and services may be provided to an employee who meets the following criteria:
 - Supports mission critical systems or provides critical campus services and is required to be available immediately both within and beyond normal business hours;

- ii. Is not normally present at a fixed workstation and/or provides support where rapid response is often required;
 - iii. Is in a role that requires frequent travel, mobile connectivity and rapid availability;
 - iv. Demonstrates a need to have mobile access to critical information and documents;
 - v. Is engaged in research activities where the device is required to meet research objectives and is an eligible research funded expense; or
 - vi. Works in situations where access to security services is otherwise limited.
- b. Mobile devices and services will not normally be issued to student employees, contract or casual employees, or consultants.

1.3 Device and Plan Selection

- a. The Vice-President, Finance and Administration shall select and manage the University's mobile device service agreement(s) and institute appropriate controls and communications.
- b. The service agreement(s) will establish a selection of mobile devices and plans from established vendor(s).
- c. The standard smart phone plan currently includes voice, data, MMS (video and picture) and text.
- d. Consideration will be given to requests from employees to use specific telephone numbers as long as the number has a local area code.
- e. Mobile devices and plans will be selected and approved by the departmental authority (Administrative Director or Dean) based on the employee's requirements.
- f. Only those mobile devices approved by the departmental authority and issued through UTS will be authorized and supported.
- g. The Vice President, Finance and Administration is the definitive authority on interpreting and administering the Mobile Devices Policy and associated Procedures and Security Standards.

1.4 Usage

- a. Mobile devices must be used and configured as detailed in the Procedures and Security Standards documentation.

Applicability of the policy

- 1.5 The Mobile Devices Policy applies to all mobile devices as well as all employees or other authorized representatives who are responsible for any mobile device issued by the University.

2. PROCEDURES

Ordering a Mobile Device

- 2.1 An employee requesting the use of a University-owned mobile device must complete a Mobile Device Request Form (online or paper copy) and submit the completed form to their departmental authority. If approved, the authorized form is to be submitted to UTS for final review and recommendation(s). The Mobile Device Request Form will require final approval from the Vice-President, Finance & Administration.

Appropriate Use

- 2.2 Employees must abide by the University's Acceptable Use Policy especially as it pertains to sensitive information as transmissions may not be secure.

- 2.3 Departmental authorities can ask to review the billing charges of their employee(s) at any time.
- 2.4 Employees are prohibited from using University-owned mobile devices for the purpose(s) of illegal transactions, harassment, or obscene behaviour, in accordance with existing University policies and government laws/legislation.
- 2.5 Employees are prohibited from using University-owned mobile devices for private commercial or consulting purposes (i.e. employee's own business).
- 2.6 Employees are expected to adhere to federal and provincial legislation governing the use of mobile devices, including during the operation of a motor vehicle. Employees charged with traffic violations for using a mobile device while driving for University business will be responsible for the resulting liabilities.
- 2.7 Mobile devices, associated accounts and all University related data are considered the property of the University and should be treated as such.
- 2.8 The University recognizes that mobile devices will incur incidental personal use. Significant personal usage (including roaming, long-distance, airtime, data and text) that exceeds the plan coverage must be reimbursed to the University by the employee.
- 2.9 Any action on a University-owned mobile device that violates the manufacturer's warranty is not condoned, and repair/replacement costs will be at the employee's expense.

Loss, Damage or Discontinued Use

- 2.10 Loss, damage or theft of a mobile device needs to be reported as soon as reasonably possible to UTS.
 - a. The cost of replacing a mobile device will be determined by contractual agreements.
 - b. The departmental authority must authorize the replacement of a mobile device.
 - c. Costs to replace lost or damaged chargers and/or cables are the responsibility of the department.
- 2.11 Departmental authorities may discontinue mobile device services at any time. Termination or change fees may be incurred and will be the responsibility of the department.

Expenses and Reporting

- 2.12 To reduce operating costs, mobile devices should use secure wireless connections where possible (i.e. secure on campus wireless, EDUROAM, secure home connections).
- 2.13 For employees with both a smart phone and tablet device, UTS strongly encourages the use of 'hot spots' as a cost effective alternative to having two mobile device plans. Approval for two plans for one employee is required from the Vice-President, Finance & Administration.
- 2.14 Monthly bills are reviewed and authorized by UTS.
 - a. Departmental authorities will be notified of overages above five dollars and the corresponding charges will be the responsibility of the employee.
 - b. The Vice-President, Finance and Administration will review the plan's monthly financial reports.
 - c. Departmental authorities are provided monthly reports upon request.

- 2.15** International travel plans must be added when travelling out of country
- a. Prior to travel, the employee must contact their departmental authority for approval.
 - b. After receiving approval, the employee must arrange through UTS to have the appropriate plan added to their package.
 - c. UTS normally requires one week's notice to process a travel package request. Requests for plan options can be sent to telephones@nipissingu.ca.
 - d. Roaming charges are the responsibility of the employee who will be travelling. If an employee incurs excessive charges, the University may request that the employee reimburse the University.
 - e. Personal travel plan costs are to be fully reimbursed to the University.
- 2.16** Personally owned devices and plans will not be reimbursed by the University.
- a. Significant cost and administrative efficiencies are achieved by incorporating all approved University mobility devices into the corporate plan.
 - b. From time to time, employees may respond from their personal device to University related texts or emails as a matter of convenience; however, this does not constitute eligibility under Section 1.2 of the policy.
 - c. Should an employee be required, for a limited period of time, to respond to texts or emails from their personal device, the University will reimburse the employee for any additional charges they incur. Depending on the nature and term of the requirement, the University may provide the employee with a reimbursement of monthly charges.
- 2.17** Device cases (i.e. OtterBox) and screen covers are highly recommended to extend the lifespan of the equipment. Product type and cost approval are the responsibility of the departmental authority.
- 2.18** Additional peripherals (i.e. keyboards) require the approval of the departmental authority with costs being the responsibility of the department.

Equipment Returns, Plan Cancellations

- 2.19** The departmental authority may request deactivation of a mobile device and terminate related services at any time.
- a. Device(s) are to be returned to UTS when the departmental authority deems there is no longer a business need.
 - b. Upon termination or resignation, an employee must return all mobile devices to UTS.
 - c. Upon retirement, at the discretion of the University and with the approval of Human Resources, an employee may have the option of purchasing their smart phone and its associated phone number at a cost determined by the University.
 - d. All returned mobile devices must be reset (erase all content and settings) and the "Find my iPhone" feature must be removed from iPhones.

3. SECURITY STANDARDS

- 3.1** UTS requires the following steps be taken to secure any University-owned mobile device upon which confidential University information may be stored:
- a. The device must require a passcode for access, preferably with a Touch ID or other biometric feature option;
 - b. Passcodes must be set to auto lock after the minimum allowable minutes of inactivity;
 - c. If mobile device is a shared/department device, the passcode must be provided to the departmental authority; and
 - d. The enabling of other security features (such as 'erase after 10 failed logins', etc.) should be considered.
- 3.2** Users are not permitted to alter University-owned devices through so called "jailbreaking" or other unauthorized modifications of the device's operating system.

Any exceptions to this policy can be made at the discretion of the Vice-President, Finance & Administration.

QUESTIONS?

1. Questions about this Policy, the Procedures or Security Standards should be directed to UTS at telephones@nipissingu.ca.
2. Questions about reimbursement procedures should be directed to Financial Services at acctpayable@nipissingu.ca.

I have received a copy of the Mobile Policy and Procedures, I fully understand the terms of these policies and procedures and agree to abide by them.

Employee Name: _____

Employee Signature: _____

Date: _____