

Policy Name:	Acquisition of Wireless Cellular Services Policy
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	April 2018
Last Updated:	September 2020
Mandatory Revision Date:	September 2025
Contact:	Chief Information Officer (CIO)

Policy:

With the increased use of mobile devices, including Bring Your Own Device, the University needs clear direction on managing the associated telecommunications expenses and security of mobile devices.

Purpose:

This policy defines the eligibility requirements for university provisioned devices, expensing of personal devices, and the associated security requirements.

Scope:

This policy applies to any instance where a mobile device uses voice or data plans through wireless providers (i.e. cellular services) and is applicable to Carleton Faculty, Staff and temporary employees.

Procedures:

Corporate Plan

Carleton University manages commercial agreements with Wireless providers. All fulltime Faculty and Staff requiring a mobile device for business purposes are required to use the University's centrally managed corporate account. Only one corporate account per wireless provider is permitted, managed by ITS.

Eligibility

Active Faculty or Staff are eligible for the corporate plan with prior written approval from their Director or delegate as indicated by the business unit Vice President.

Part time, Casual, or Term employees are not eligible for University funded mobile device nor for the Corporate plan. With prior written approval from the hiring Director or equivalent level, part time, Casual and TERM employees are permitted to expense a portion of their personal mobility plan, up to maximums as identified by Carleton University in the Terms and Conditions.

Mobile devices and mobility plans supported by internal and external research grants or contracts must comply with Carleton University's Research Expenses Guidelines. Specific funding agency rules and regulations may take precedence and should be consulted.

Jail Broken or *Rooted* devices will not be eligible for the corporate account nor reimbursement and are prohibited from use with university enterprise services such as email.

To protect the University, mobile devices that are covered by this policy must comply with the University's *Mobile Technology Security Policy*. Mobile devices must be running ITS managed Mobile Device Management Software.

Personal Use

Carleton University permits the use of a Corporate Device for personal use providing it is in accordance with the Carleton University *Acceptable Use Policy for Information Technology (IT)* and any costs or surcharges associated to the personal use including, but not limited to personal long-distance calls, are reimbursed to the university.

Termination/Resignation

Upon termination or resignation of Faculty or Staff, the device remains the property of Carleton University and must be returned to ITS or the original purchasing department. The mobile phone service will be put on hold. At the agreement of the purchasing department, the departing individual may opt-in to purchasing the phone. Failure to return the phone will result in being billed for the current market value of the phone and remote wipe of the phone.

Terms and Conditions

The University has set of terms and conditions that include but are not limited to:

- Maximum reimbursement limits for personal devices
- Porting of phone numbers into and out of the university's Corporate plan
- National and International packages
- Device Damage

See <https://carleton.ca/mobileservices/mobilityterms/> for the complete list of terms and conditions.

Roles and Responsibilities

All users of mobile devices are responsible for:

- Ensuring reasonable measures are taken to protect the device from physical damage or theft
- Ensuring that safeguards and protection mechanisms intended to protect data on mobile technologies are not tampered with or modified
- Immediately reporting the loss or theft of a mobile device to the ITS Service Desk

ITS is responsible for:

- Management of the wireless provider account
- Inter-departmental billing
- Management of the Mobile Device Management offering

Directors (or equivalent) in all Departments are responsible for:

- Approving the provisioning for mobile devices
- Ensuring that University-owned mobile devices are returned to the University on departure from employment

Human Resources is responsible for:

- Reporting employee departures to ITS to ensure that mobile access to University infrastructure is disabled

Compliance

Non-compliance to this Policy may result in disciplinary action.

Contacts: Chief Information Officer, ITS

Links to Related Policies:

<http://www.carleton.ca/secretariat/policies/>

- Acceptable Use Policy for Information Technology (IT)
- Mobile Technology Security Policy