Northeastern University

Policy on Mobile Devices

BUSINESS AND FINANCIAL AFFAIRS

Effective Date: July 1, 2015

Date Revised: October 16, 2017

Supersedes: N/A

Related Policies:

- **Policy on Appropriate Use of Computer and Network Resources**
- **Policy on Confidentiality of University Records and Information**
- **Policy on Student Rights under the Family Educational Rights and Privacy Act (FERPA)**

Responsible Office/Department: Chief Financial Officer

Keywords: Cell phone, mobile device, data security

I. Purpose and Scope

The purpose of this policy is to establish a framework for consistent decision-making regarding the provision of essential, business-related mobile devices to Northeastern University (the "University") faculty and staff. University leadership intends that this policy, and its associated procedures as incorporated by reference, will promote compliance with Internal Revenue Service requirements and manages the risks and administrative burdens associated with the use of mobile devices to facilitate University business.

II. Definitions

Mobile telephone: A portable device that connects to a mobile network for the provision of voice, text, and multimedia messaging services, as well as (in some cases) data connectivity.

Smartphone: A type of mobile telephone that has data connectivity for email access, calendar management, and web browsing capabilities, as well as the capability to run numerous applications.

Mobile device: A portable device that connects to a mobile network for the provision of voice, messaging, and/or data services. Examples of cellular devices include mobile phones, iPads, and modems allowing laptops to connect to mobile data networks.

Senior Leadership Team (SLT) Member: The most senior leader of one or more Division(s), that reports directly to the University President.

Division: Operational unit as defined by the University's organizational structure. An SLT Member is accountable for one or more Divisions in their portfolio of responsibility.

Device Manager: The individual that has stewardship responsibility for the Mobile Devices, Mobile Telephones, and Smartphones of the Division, as delegated by the SLT Member.

University-owned device: A mobile device purchased and owned by the University that connects to a mobile network through a University-sponsored plan.

University-sponsored plan: A contract between the University and a mobile service provider to provide voice, messaging, and/or data connectivity to a University-owned device.

Device Applications, or "Apps": A self-contained piece of software designed to fulfill a particular purpose; an application. For the purposes of this policy, the definition applies as, downloaded by a user to a mobile device.

Communication reimbursement: A monthly reimbursement for device expenses.

Personal mobile device: An employee-owned mobile device, rather than the University. The device that connects to a mobile network through a personal or a University-sponsored plan.

Personal mobile plan: A contract between an employee and a mobile service provider to provide voice, messaging, and/or data services to a personal mobile device.

Personal use: Usage of a University Sponsored Plan for non-university business.

Eligible employee: An employee of the University who meets the requirements set forth below to receive either a University-owned device or a communication stipend.

III. Policy

1. *Eligibility to receive a university-Owned Device or a Communications Reimbursement*

Each Division's SLT representative decides whether employees are qualified to receive either a University-owned device or a communication reimbursement (reimbursement is by exception only). The qualification criteria are:

- The nature of the employee's job requires that the University be able to contact the employee, via voice or access to other communication / connectivity needs such as text, email, mobile applications, or data at all times for work-related matters; OR
- The nature of the employee's job requires that the employee be accessible to co-workers for work-related matters either:
    - When the employee is away from the employee's office, OR
    - Outside of the employee's normal work hours.

Enablement with a University Sponsored Service, using a University Owned Device, is the approach that is strongly preferred. A University reimbursed personal mobile device and/or personal mobile plan is an exception to policy. As such, an employee must receive written approval to a request made to the employee's responsible SLT member.

2. *Policy on University-Owned Devices*

The required method of enabling eligible employees with mobile communication services is via University-owned devices on University-sponsored plans. The University purchase devices directly from the carrier and pays for the related monthly service for employees in positions that leadership deems fit the characteristics in Section 1 above.

As with any device that has the capability to store data, or access data via the University network or the Internet, it is the employee's responsibility to:

- Adhere to University data security policies, available on the Policy webpage and at SecureNU
- Maintain a current back up of the device to prevent the possible loss of data

These responsibilities apply whether the device is University owned, or a personal mobile device.

3. *Device Replacements and Upgrades*

Replacement of lost, stolen, or damaged University owned devices occurs when reasonably necessary. If an employee fails a reasonable standard of care for devices, it is

the immediate supervisor's decision whether to replace or not. The employee must secure approval from their direct supervisor for a replacement device prior to initiating the replacement transaction from the carrier. Failure to do so could result in the replacement cost being an employee responsibility.

Device upgrades must be in accordance with upgrade offers embedded within University sponsored plan and its related upgrade cycles unless otherwise approved by the responsible SLT member. The employee's direct supervisor has the discretion to approve in plan upgrades, and approval must occur before contacting the carrier for the upgrade. Otherwise, the employee is at risk of potentially being responsible for the cost of the upgraded device.

4. *Device Disposal / Recycling / Reassignment*

When a decision has been reached to disposed of a University-owned device, the Division's Device Manager must send the old device to ITS.

University policy strongly recommends that the Division Device Manager request the return of device peripherals (cases, chargers, headphones, etc.) with the device for recycling / reassignment if purchased with University funds. Central administration will retain any funds received from the recycling vendor, to support the costs of the mobile device program. Please reference the Procurement Services website for additional details about device recycling and / or disposal.

In situations of unplanned cessation of service (e.g., termination of employment, termination of eligibility, etc.) a device may have a remaining useful life. If the Division's Device Manager determines that reassignment is the best value option, the Device Manager is responsible for sanitizing the device of all user data by performing a system reset as described in step 3 above. ITS has no role in the reassignment process.

5. *Policy on Personal Usage and Personal Apps*

Policy allows for reasonable personal usage of University Managed Service, or of a service supported by reimbursement for a personal mobile plan. Supervisory judgment defines "reasonable" on a case-by-case basis given work and employee circumstances. This policy expects that supervisors evaluate usage patterns during the annual service recertification process. Personal usage of a University Managed Service that results in a fee (e.g., download of apps, minutes/data overages) is the responsibility of the employee and must be reimbursed to the University in the month following billing. There is no expectation that employees reimburse the University for personal usage of

University Managed Service if charges remain less than or equal to the standard monthly fee.

Policy prohibits employees from purchasing "apps", music, or other content for personal use with a University account. If this activity occurs, the employee must provide evidence of reimbursement of these costs. When purchasing "apps" for personal use, employees must use their personal iTunes, Google Play, etc. accounts. It is at the supervisor's discretion whether an "app" purchased in this fashion qualifies for a business purpose, and as such is eligible for reimbursement by University funds.

6. *Retention of Personal Telephone Numbers Used on NU Service Accounts*

Employees that wish to assign, and later retain, a personal mobile device number to a University-managed account must make this known when initiating service. The University cannot guarantee that the employee will be able to retain the telephone number on termination of employment. To retain a personal mobile device number, the employee must secure approval from the Divisional Device Manager before initiating mobile device service. Reassignment of the personal number from an NU-sponsored account to a personal account must occur at the time of cessation of employment. Otherwise, the personal number may be lost at the time of transition. Employees that wish to initiate an account with a personal number should discuss this with their Divisional Device Manager.

7. *Process on Reimbursement for Mobile Service Costs*

This section of the policy only applies if an employee has received exception approval as defined in section 1 of this policy. Once approved, the employee will request reimbursement on a monthly basis and submit the statement from their carrier as proof of service. Said reimbursement shall not exceed the total monthly cost of a standard University-sponsored plan. The cost of such plan will be determined at the beginning of each fiscal year.

Eligible employees, approved for a communication reimbursement shall be responsible for the purchase and upgrade of their own personal mobile device in accordance with Section 9 of this policy. The University will not replace personal mobile devices for any reason (e.g., loss, theft, or damage).

8. *International Usage of Mobile Devices*

When the annual eligibility is determined for University Sponsored Service, the Division should indicate the need for routine international service at that time. In the event that work responsibilities change (temporarily or otherwise) to require international device connectivity, the employee must initiate the following process to avoid personal liability for international device charges:

- Contact immediate supervisor with a request for international service. The request must allow enough time for supervisory approval *plus 24 hours for the wireless carrier to initiate service prior to international* usage.
- Once approved, the employee must request international service from their Divisional Device Manager. The request must include the dates service is required, and if known, the countries in which the service will be used.

- A failure to initiate international service before usage will result in unauthorized charges under this policy. As such, these charges will become the employee's personal financial responsibility.

9. *Security Requirements for Mobile Devices*

Several related documents define security standards in both general guidelines, and specifics tailored to mobile devices:

- Policy on Enterprise Passwords

- Policy on Appropriate Use of Computer and Network Resources

- Procedure Supporting the Cellular Telephone and Mobile Device Policy

10. *Personal Mobile Device Topics*

Users that receive approval to use a Personal Mobile Device from their SLT member must comply with device compatibility and security standards. SLT approval does not extend to the type of device used to connect to NU computing resources. ITS evaluates mobile devices on a routine basis and lists devices qualified to connect to the NU network. Employees that choose to connect non-compliant devices are in direct violation of this policy and may be subject to disciplinary action.

11. *Procedures*

The Northeastern University Procedures Supporting the Policy on Mobile Devices provide detailed information and requirements that are as binding as the policy itself.

IV. Additional Information

Failure to adhere to the standards established in this policy and its related procedures can result in disciplinary action ranging from loss of University-sponsored CT&D service to termination of employment, depending upon the severity of the violation.

V. Contact Information

1.) For questions about data security or quality of cell service, please contact ITS at 617-373-4357 (xHELP) or reference the FAQ s.

2.) To Accounts Payable at x2652 for status on approved invoices that have not yet been paid.