Policy Name: Mobile Communications Device Policy

Policy Owner: Georgia Tech Cybersecurity

Policy Contact: Joe Lewis, Chief Information Security Officer, ask@security.gatech.edu

Reviewed By: Office of Information Technology, Cyber Security, Office of the General Counsel, Business Services, Controller's Office, Accounts Payable, Georgia Tech Research Institute, College of Lifetime Learning, Internal Audit

Policy Steering Committee Approval: February 2026

Policy Purpose: This existing policy has been updated to clarify requirements for GT-owned mobile communications devices (MCDs) to ensure they follow University System of Georgia's IT Handbook Section 8: Mobile Device Management. The policy updates also clarify how MCDs are to be acquired, managed, and used across the Institute, and what, if any, reimbursements are allowed.

Summary of Substantive Policy Changes:

- Throughout, removed references to "wireless" or "wcd" and changed to "mobile" or "mcd".
- Page 1, added a the reason for the policy and additional in scope or out of scope items that this policy will cover.
- Page 2, edited responsibilities of units and specified where inventory of MCDs will be. Additionally, rewrote the criteria to determine business need for a unit providing a mobile device to an employee.
- Page 3, removed reimbursement for privately-owned mobile devices/services.
- Page 4, added the scope and additional definitions and clarified the responsibilities for units, employees, and OIT.

Georgia Institute of Technology

Mobile Communications Device Policy

Policy No. 14.1
Type of Policy: Administrative
Effective Date: January 2005
Last Revised: TBD
Policy Owner: Georgia Tech Cybersecurity
Policy Contact: Joe Lewis, Chief Information Security Officer, ask@security.gatech.edu

1. Reason for Policy

This policy outlines requirements for Institute owned mobile communication devices (MCDs) to ensure they are acquired, managed, and used in a manner that supports operational efficiency, safeguards institutional data, and complies with financial, regulatory, and cybersecurity requirements. Establishing clear standards for issuing, monitoring, and securing these devices helps Georgia Tech uphold responsible stewardship of resources while enabling employees to perform their duties effectively.

2. Policy Statement

It is the responsibility of Georgia Tech and each of its budgetary units to implement procedures to issue and use mobile communication devices and services in the most cost-effective manner. Heads of budgetary units (Vice Presidents, Deans, School Chairs, Unit Heads) or their designee are authorized to approve the acquisition of mobile communication devices and services. Mobile Communication Devices (MCDs) for this policy include, but are not limited to, mobile phones (smartphones or not), tablets with mobile data, and hotspots or other devices with mobile service. By contrast, cordless telephones, VoIP Phones, tablets without data plans, Internet of Things (IOT) devices, computers or laptops with Wi-Fi or wired connections, and other devices are not covered by this policy.

Guidelines for Acquisition and Use

An Institute-issued MCD may be a suitable resource to conduct Institute business

when it enhances performance or when it is proven that an employee cannot perform their duties without an MCD. The individual units are responsible for:

- Determining the business case for the use of MCDs and services.
- The justification and approval for each MCD and service issued or approved.
- Monthly review of MCD bills and usage by a unit manager or delegate.
- Wiping and sanitizing MCD prior to repair, reissue, or disposal.
- Ensuring all MCDs are inventoried in a Georgia Tech approved central inventory system.
- Ensuring all devices are enrolled in an authorized Mobile Device Management (MDM) solution.
- Maintaining current inventory of MCDs in the central Configuration Management Database (CMDB).

Criteria for Determining Need

A unit may acquire an MCD for an employee when communication needs cannot be met with other available devices such as standard telephone equipment or soft client. Examples of conditions under which a unit may obtain an MCD and service include:

- The employee's position requires them to maintain information or communicate with others to perform their job functions.
- The organization provides additional protection to the employee when they work in potentially hazardous conditions.
- The employee cannot adequately meet communication requirements using other available alternatives, such as a standard telephone line or soft client.
- On-call personnel must be available to respond to critical system failures or service disruptions.
- The organization uses this as the most appropriate means to respond to campus emergencies or to achieve business efficiencies.

The unit head (or designee) of employees using Institute owned MCDs is responsible for determining the business needs and selecting an appropriate mobile service package that meets these needs.

Personal Usage

MCDs assigned to faculty or staff members are for official Institute business. While incidental personal use may occur, this use should not result in additional charges to the Institute. If personal use results in additional charges to the Institute the faculty or staff member must notify their unit head or supervisor and reimburse the Institute for charges incurred in the use of the device. Reimbursement to Georgia Tech for personal use of any MCD should be deposited with the Bursar's Office by the unit, along with a copy of the annotated bill noting the personal communications and

cost.

Ordering and Payment Administration
The following ordering and payment processing options shall be used for all MCDs issued. MCD's should be procured by the unit through existing Georgia Tech approved mobile contracts. In special circumstances, Procurement may utilize other agreements obtained from any carrier that best meets the Institute's needs.

- Institute-Owned MCDs and Service
  For positions meeting the requisite criteria, the Mobile Phone Service Request form should be completed by the employee, approved by the direct manager, and have prior financial approval. Once approved, units should acquire MCDs and services via their unit PCard or Supplier Invoice Request (SIR), after completing any necessary forms provided by the service vendor representative to establish legitimate Georgia Tech service account(s). Only designated Georgia Tech Procurement officials may enter into contracts on behalf of Georgia Tech, and any actual contracts should be forwarded to Procurement for review and signature. Any contracts signed by an unauthorized employee are personal obligations of the employee.
- GT Employees (faculty and staff) are not eligible for reimbursement of a personal MCD. For additional guidance, please refer to the following policies:
  - Georgia Tech Policy 5.2.1.5 – Reimbursement for Purchases Made Using Personal Funds
  - Department of Administrative Services - Statewide Telework Policy

Right to Monitor Communications
Georgia Tech reserves the right to investigate, retrieve and read any communication or data composed, transmitted or received through its voice services, online platforms, and/or stored on its servers and/or property, without further notice to employees, to the maximum extent permissible by law. For additional information, please see Open Records Act Policy.

3. Scope
This policy applies to all Institute employees and affiliates.

4. Definitions

Configuration Management Database (CMDB)	A centralized repository that stores information about Georgia Tech's IT assets, including their attributes, relationships, and dependencies.

Endpoint Management Tool	A centralized platform used to monitor, manage, and secure endpoint devices across Georgia Tech. (e.g., JAMF, Intune, or Workspace One)
Mobile Communications Device (MCD)	Phones or tablets running iOS or Android systems, hotspots, and devices with a data plan.
Mobile Device Management (MDM)	A set of technologies and administrative processes used to manage, monitor, and secure mobile devices at Georgia Tech.
Mobile Services	Voice, text, data, and/or international plan
Soft Client	Software or app that can be operated on a computer, smartphone, or tablet to make and receive telephone calls and/or messaging.

5. Responsibilities

Units are responsible for:

- Determining the business case for the use of MCDs and services.
- The justification and approval for each MCD and service issued or approved.
- Monthly review of MCD bills and usage by a unit manager or delegate.
- Wiping and sanitizing MCD prior to repair, reissue, or disposal.
- Ensuring all devices are enrolled in an authorized Mobile Device Management (MDM) solution.
- Ensuring all devices are inventoried in a Georgia Tech approved central inventory system.
- Maintaining current inventory of MCDs in the central Configuration Management Database (CMDB).

The Office of Information Technology is responsible for:

- Establishing an inventory for MCDs in a campus approved inventory system

The individual assigned a MCD (primary user) is responsible for:

- Ensuring the MCD is used for official Institute business.
- Using reasonable care to prevent damage to or loss of the MCD.
- Reporting personal usage that results in additional charges to the Institute.
- Reviewing the export control policy prior to leaving the United States.
- Completing an annual data certification from a central GT inventory system for any Georgia Tech owned mobile device.
- Returning the MCD to unit manager or delegate when transferring units, terminating employment with Georgia Tech, or when the use is no longer required for the position.

- Complying with the password policy.

6. Enforcement

Unauthorized use of MCDs or services, failure to repay the unit for personal charges, or other policy violations may result in suspension of MCD use and disciplinary action as necessary.

To report suspected instances of ethical violations, please visit Georgia Tech's Ethics Hotline a secure and confidential reporting system, at: https://secure.ethicspoint.com/domain/en/report_custom.asp?clientid=7508

7. Related Information

Acceptable Use Policy
Cybersecurity Policy
Personal Information Privacy Policy

8. Policy History

Revision Date	Author	Description
TBD	OIT	Updated to clarify responsibilities, terminology, and reimbursement for personal devices
July 2021	OIT	Editorial Updates
January 2005	OIT	New Policy