



Policy Title	Cellular, Wireless Communications Devices, and Services Policy
Issue Date	January 1, 2017
Effective Date	September 1, 2024
Last Updated	August 1, 2024
Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: <a href="mailto:ocs@kennesaw.edu">ocs@kennesaw.edu</a>

### 1. Policy Purpose Statement

Kennesaw State University (KSU), at its discretion, may provide wireless voice and data services (e.g., cellular services) and associated devices, where doing so would enhance job performance, in accordance with specific criteria, including being the most appropriate and cost-effective method of achieving business needs.

### 2. Background

The Georgia Technology Authority Office of Planning and Budget policy memorandum No. 4 states:

It shall be the responsibility of each State agency to manage and minimize the costs of using telecommunications services and equipment. This policy applies to all State departments, institutions, boards, bureaus, agencies, authorities, colleges and universities (all are which hereinafter referred to as “agency” or collectively as “agencies”). Each agency shall develop a telecommunications policy based upon the guidelines established in this statewide policy.

Agencies will be responsible for maintaining adequate documentation to ensure that these guidelines and criteria have been met.

### 3. Scope (Who is Affected)

This policy covers anyone who uses University wireless devices and voice/data services or approves and supervises the use of wireless devices and voice/data services. The scope of wireless devices and voice/data services are as follows.

- Individual use wireless devices, such as cellular and satellite phones, hotspots, tablets, laptops, or other devices capable of using metered voice and/or data services that incur costs to the institution.
- Voice and data services that are not provided as part of the standard campus telecommunications infrastructure and incur additional cost to the University (e.g., cellular services, satellite phone services, or other services which incur charges based on a per-unit measure, such as minutes consumed, or data transferred).

#### 4. Exclusions or Exceptions

None.

#### 5. Definitions and Acronyms

**Wireless Device:** A device (often mobile) that receives and/or transmits using wireless technology, such as cellular, satellite, or radio frequency (RF) communications.

**Wireless Voice and Data Service:** Communications service that is not provided as part of the campus telecommunications infrastructure and incur additional cost to the University (e.g., cellular services and satellite phones).

**Tethering:** Allowing one or more devices to receive data services by sharing the data service provided by another device.

#### 6. Policy

University provided wireless devices and wireless voice and data services may be allowed, when it can be justified based upon a business need, such as a requirement to perform job functions or resulting in a significant improvement in job performance that enhances the University mission.

##### a. Supervisor/Unit/Department Responsibilities

The employee's unit head (or designee) should evaluate the business need and submit a request with justification to their corresponding vice president or dean for approval. Vice presidents and deans must evaluate and provide their approval based on their evaluation of legitimate business use and cost effectiveness, in alignment with the examples in section 6b.

Devices and services used in support of research must have the additional approval of the Chief Information Security Officer.

The employee's supervising unit or department is responsible for:

- Evaluating the business need (see Section 6b) and maintaining a record of vice president/dean approvals;
- Maintaining an inventory of devices and active services for each employee or unit;
- Monthly monitoring of appropriate use, including call activity and data plan usage that may be personal, excessive, inappropriate, or incur unnecessary cost to the University;
- Discontinuing service and recovering devices in a timely manner (30 days) when an employee separates or the business need can no longer be justified; and
- Performing an annual review of active devices, services, and service levels.

Inventory of devices and services must include the assignee (individual or organizational unit in the case of a shared device/service), any assigned telephone numbers, and serial numbers of university-owned devices associated with the service. This inventory must be current and made available upon request by KSU administration.

##### b. Criteria for Determining Need

Departments may request a wireless device and/or wireless voice and data service for any employee where communication needs cannot be met by less expensive alternatives. Approval is based on an evaluation of the most appropriate and cost-effective method of

achieving business needs.

Examples of conditions under which services and devices may be approved are:

- Directly enhances an employee's job responsibility of protecting the lives of others;
- Is required for an employee to respond to environmental emergencies;
- Is required for the protection of the employee in potentially hazardous working conditions;
- Regular requirement for two-way real-time communication where stationary voice and data communications cannot be made available (e.g., construction areas);
- Frequent travel requirements (e.g., >25%) across a large geographic area where a considerable amount of time is spent away from the institution or in transit and the employee is required to have access to the Internet and/or stay in contact with the institution or institutional affiliates;
- Required to participate in a Wireless Priority Service (WPS) as a part of their job responsibilities;
- Required for individuals who play a critical role in campus emergency and disaster response operations; and
- Directly supports the institution's need to remediate disruptions to critical (24x7) campus services;
- For use in academic instruction (where not duplicative of already provided UITS services);
- To support approved research (requires additional approval from the Chief Information Security Officer).

### **c. Employee Responsibilities**

Employees in possession of a University provided wireless device and/or wireless services are responsible for:

- Promptly notifying their department when a device or service is no longer necessary to support the business need;
- Promptly notifying their department when a device is lost, stolen, or damaged;
- Limiting personal use of University provided wireless services and reimbursing for costs associated with personal use; and
- Minimizing costs associated with the use of University provided wireless services.

Devices supplied by the University remain the property of the University and must be returned upon termination of employment or upon request. If an employee fails to do so, that employee will be charged for replacement equipment at the time of separation.

### **d. Personal Use of University Provided Mobile Voice and Data Services**

Mobile voice and data services are provided for official business use. Incidental personal use is allowed, as long as it does not incur additional costs for the University and does not violate University usage policies. If personal use results in additional service charges, the employee is to notify their unit/department and reimburse the University for overages. An annotated copy of the invoice, noting all personal usage and costs, should be provided to the Bursar, along with payment.

### **e. Use of Personally Owned Wireless Devices or Services for Business Purposes**

Departments may choose to have the University provide mobile voice and data services for

use on an employee's personally owned device. Under no circumstances will the University buy out personal service contracts. The employee is responsible for meeting all personal contract obligations.

Occasional use of personally owned voice and data services, in line with the criteria outlined in Section 6a may be approved for reimbursement by the unit/department at the unit/department head's discretion. Reimbursements are limited to the total overage charges shown on the employee's monthly invoice; in excess of minutes and metered services included in the employee's personal service plan. The employee is responsible for making personal payment to the provider, as per employee/service provider agreements.

#### **f. Obtaining a Mobile Wireless Device for Business Use**

A department/unit has the following options when determining the most appropriate solution for meeting business needs.

- A department may select from any of the lowest cost wireless devices being offered by the University. In this scenario, the device remains the property of the University and must be surrendered on separation or at the request of KSU administration.
- A department may allow an employee to receive University mobile voice and data services on their personally owned device.
- Devices must be carrier unlocked and be models that are currently offered and supported by university service providers. Activating university voice and/or data services on a personally owned device will be done on a best-effort basis.

#### **g. International Roaming and Usage Charges**

In order to manage and minimize mobile voice and data service costs, employee's using either University provided services or seeking reimbursement for business use of non-University services, must temporarily adjust their service plans or purchase calling cards, in anticipation of international travel. Reimbursement for international roaming charges may be denied if no action is taken on the part of the employee to minimize costs. Employees who travel internationally with high frequency may receive approval for a continuous international service level on their University provided mobile voice and data services. Departments are responsible for roaming and overage charges their employees incur during international travel.

#### **h. Tethering Devices and Services**

Where a business need exists, departments may allow employees to tether laptops and other devices to their University provided data service. This is preferred over providing an employee with multiple data services that incur a higher cost.

#### **i. Security of Mobile Voice and Data Communications**

Security of confidential/sensitive University information is paramount. Sensitive communications should be conducted through the most secure means possible. This includes using the most secure device, service configurations, and protocols. Use of the University VPN is highly recommended. Units are responsible for determining the level of security required to meet their business objectives and bear the risks associated with security related decisions.

Kennesaw State University  
Policy: Cellular, Wireless Communications Devices, and Services Policy  
KSU Policy Category: Information Technology

Page 6 of 6

## 7. Associated Policies/Regulations

- a. [Georgia Technology Authority, Rules, Regulation and Procedures Governing the Acquisition and Use of Telecommunication Services and Equipment](#)
- b. [USG Information Technology Handbook](#), Section 5.4, USG Information Asset Management and Protection

## 8. Procedures Associated with this Policy

There are no procedures associated with this policy.

## 9. Forms Associated with this Policy

There are no forms associated with this policy.

## 10. Violations

Individuals and KSU employees who are found to be in violation of this policy are subject to a range of sanctions, including but not limited to denial of services covered by this policy, disciplinary action, dismissal from the University, and/or legal action.

## 11. Review Schedule


The Office of Cybersecurity will review the Cellular, Wireless Communications Devices, and Services Policy annually.

---

At Kennesaw State University, institutional policies that have undergone the established shared governance review and feedback process are presented to the President and Provost for final approval. The signatures below indicate this institutional policy has been reviewed and approved by the President and Provost.

DocuSigned by:  
  
October 28, 2024  
11EA3F49C7FD4B9...

Dr. Kathy S. Schwaig,  
President  
Kennesaw State University

DocuSigned by:  
  
October 28, 2024  
26412C41D0DE4E2...

Dr. Ivan Pulinkala,  
Provost and Executive Vice President for  
Academic Affairs  
Kennesaw State University