ADMINISTRATIVE DIVISION FINA Administration and Finance		**POLICY NUMBER** FINA 2.30 (formerly FINA 7.08, BUSF 7.08)
POLICY TITLE Wireless Communication Stipends		
SCOPE OF POLICY USC System	**DATE OF REVISION** 09/01/2024	
RESPONSIBLE OFFICER Executive Vice President for Finance and Chief Financial Officer	**ADMINISTRATIVE OFFICE** University Finance – Controller's Office	

PURPOSE

~~The purpose of this~~This policy ~~is to~~ addresses the payment of wireless communication fees incurred by University employees while conducting University business and to establish consistent standards to be applied to all units.

DEFINITIONS AND ACRONYMS

Stipend – A fixed sum paid periodically to an employee to defray personal communication device expenses when such devices are used, in part, to fulfill work-related activities.

POLICY STATEMENT

The University may provide a stipend to an employee who has an official business need for a wireless communication device and receives appropriate approval for such a stipend. The respective unit/department is responsible for documenting appropriate justification.

A. Eligibility

To qualify for a wireless communication stipend, the employee must have a business need. Examples of a qualifying business need may include:

- The job function requires the employee to work regularly in the field and be immediately accessible.
- The job function requires the employee to be immediately accessible outside of normal business hours.
- The employee is responsible for critical infrastructure and needs to be immediately accessible at all times.
- The employee travels regularly and needs to be accessible and have access to information technology systems while traveling.
- Access to a wireless communication device would, in the judgement of the supervisor and department head, render the employee more productive and effective.

B. Requirements and Restrictions

Stipends are funded by the unit/department through an appropriate funding source. Sponsored awards may not be used to pay for wireless communication stipends unless specifically authorized by the sponsor. Misuse or fraudulent receipt of a wireless communication stipend may result in administrative and/or disciplinary action.

The wireless communication stipend is intended to reimburse the employee for the business use of the device. It is not intended to fund the cost of the device or pay for the entirety of the monthly bill. The assumption is that most employees also use their wireless communication devices for personal calls. The employee is not required to maintain a log for business and personal usage when receiving a stipend.

Cell phones and other wireless devices should not be selected as an alternative to other means of communication (e.g., landlines) when those methods would provide adequate but less costly service to the University. An employee ceases to be eligible for the stipend when their job duties change and no longer support a business need for a wireless communications device or when the employee terminates employment with the University.

The wireless communication stipend does not constitute an increase to base pay and is not included in the calculation of percentage increases to base pay due to raises, job upgrades, retirement, or other compensation increases. Wireless communication stipends are not subject to tax withholding. When employees are required to use their personal cell phones for business purposes (non-compensatory business use), the stipend is considered non-taxable.

C. Employee Responsibilities

When a wireless communication stipend has been approved and provided to an employee for the conduct of official business, the employee is responsible for the following:

- Providing the phone number associated with the device and being available for calls during those times specified by the supervisor or department head,
- Selecting a wireless carrier whose services meet the requirements of the job responsibilities,
- Informing the University when eligibility criteria are no longer met or the wireless service has been cancelled,
- Complying with all laws regarding use of devices while driving (the University will not be liable for noncompliance),
- Providing copies of the associated phone bill upon request,
- Using discretion in relaying confidential information over wireless devices, and
- Obtaining technical support from the vendor providing the phone.

D. Security

The University reserves the right to require any mobile device accessing the University's infrastructure to be subject to the University's data and security requirements, standards, and guidelines. Security policies may include device requirements for mobile anti-virus/spyware, mobile firewall, secure communications, encrypted file folders, strong passwords, two-factor authentication, and/or destruction and disability in the event of a lost or stolen device or termination.

E. University-Issued Wireless Communication Device

While the issuance of stipends for business use of personal devices is the preferred approach, an employee may be issued a wireless communication device by the University in rare instances. Issuance of a University cell phone requires appropriate justification and approval.

Existing state term contracts must be used to purchase wireless communication devices. Regardless of funding source, devices purchased through the University are the property of the University and must be accounted for as required by State law and turned in when an employee transfers or terminates. Service plans should be reviewed on at least an annual basis to ensure the level of service is still justified.

Personal use of University-issued devices is strongly discouraged. Calls and communications on University devices should be kept brief to ensure efficient use of University resources. It is the responsibility of the department head to monitor usage to ensure abuse does not occur. University-owned devices may be revoked if there is evidence of abuse or misuse. The employee will be responsible for reimbursing the University a portion of the cost if unnecessary or excessive personal use occurs. Devices should be kept secure to prevent unauthorized use. When loss or theft occurs, a police report must be filed to account for the loss of state property and the University Controller and the University Information Security Office must be notified promptly.

F. Freedom of Information Act

Regardless of whether a stipend is provided, the personal devices of University employees are subject to disclosure under the Freedom of Information Act if such devices are used for business purposes (e.g., sending and receiving messages involving University business).

PROCEDURES

The accompanying procedure provides additional details on the administration and management of this policy. The procedure can be found here:
https://sc.edu/about/offices_and_divisions/controller/toolbox/policies_and_procedures/index.php

RELATED UNIVERSITY, STATE, AND FEDERAL POLICIES

FINA 1.00 – Chart of Accounts

FINA 2.12 – Accounts Payable
FINA 2.14 – Acquisition and Payment of Goods and Services
FINA 2.82 – Asset Management
FINA 3.00 – Sponsored Awards
HR 1.39 – Disciplinary Action and Termination for Cause
IT 1.00 – Information Technology Procurement
IT 3.00 – Information Security
LESA 5.10 – Enterprise Risk Management
UNIV 1.51 – Data and Information Governance
UNIV 1.52 – Responsible Use of Data, Technology, and User Credentials
UNIV 1.60 – HIPAA Compliance
UNIV 2.00 – Freedom of Information

HISTORY OF REVISIONS

DATE OF REVISION	REASON FOR REVISION
09/01/2024	Language, content, and formatting updates
09/24/2020	Policy reviewed and updated as appropriate.
09/8/2010	Policy revised to reflect policy category change from (from IT to BUSF). Policy organization, content and accuracy reviewed; no substantive revisions required.
???	Policy creation.

~~ADMINISTRATIVE DIVISION~~ ~~FINA Administration and Finance~~	~~POLICY NUMBER~~ ~~FINA 7.08 (formerly BUSF 7.08)~~
~~POLICY TITLE~~ ~~Cellular and Wireless Telephones and Devices~~	
~~SCOPE OF POLICY~~ ~~USC System~~	~~DATE OF REVISION~~ ~~September 24, 2020~~
~~RESPONSIBLE OFFICER~~ ~~Vice President for Finance and Chief Financial Officer~~	~~ADMINISTRATIVE OFFICE~~ ~~University Finance - Controller's Office~~

~~PURPOSE~~

~~It is the policy of the University to provide the equipment, services, and other resources necessary for its faculty and staff to discharge their job-related responsibilities properly. Cellular and wireless telephones and devices may be included among these resources. For the purposes of this policy, cellular and wireless telephones and devices are hereinafter referred to as "eDevices."~~

~~POLICY STATEMENT~~

It is the responsibility of the vice president, dean, or director to justify the need for an employee under his or her management to have an eDevice. Justification could be based on increases in efficiency, effectiveness, or enhancement of personal employee performance. For academic units, approval is required from the Dean. For administrative or service units, approval is required from the Director or Vice President. For the purposes of this policy, a unit is defined at the responsibility level. Departments are required to document and maintain the approval and justification for each user in local area work files.

PROCEDURES

A. eDevices that store, process or transmit university data are subject to all data and security requirements, standards and guidelines as described in related university policies, such as: UNIV 1.51, UNIV 1.52, UNIV 1.60, IT 1.00 and IT 3.00.

B. The University discourages use of agency eDevices for personal use. However, if circumstances should require an individual who is assigned an eDevice to use the eDevice for personal use, then that portion of the cost of the personal eDevice air time that causes the service bill to exceed the allotted monthly air time should be reimbursed to the University. As such, it is the responsibility of the vice president, dean, or director to monitor eDevice usage to ensure that abuse does not occur. The use of University- owned eDevices by faculty or staff may be revoked if there is evidence of abuse or misuse.

C. eDevices purchased through the University, regardless of the source of funds, are the property of the University. eDevices, accessories, and equipment must be accounted for 2 as required by state law, and are to be turned in to the department when an employee transfers or terminates. When an eDevice is replaced, the old eDevice must be turned in to Consolidated Services. See University Policy BUSF 5.00 Property Accountability for inventory and tagging requirements.

D. If an eDevice is lost or stolen, a police report must be filed to account for the loss of state property, and the University Information Security Office must be notified if the eDevice was used to store, process or transmit university data to determine if additional actions may be required to protect access to university data or resources. If an eDevice is damaged or lost, the vice president, dean, or director, at his or her discretion, may require the employee to pay for a replacement eDevice.

E. Calls or other communications on University eDevices should be kept brief to ensure efficient use of University resources. eDevices should be kept secured to prevent unauthorized use. Each area is responsible for the payment of expenses associated with eDevices used by that area.

F. The use of eDevices while driving on University business is strictly prohibited.

G. Service plans (coverage and minutes of airtime) should be selected carefully to meet

the needs of the respective areas. These plans should be reviewed at least on an annual basis to ensure the need for the level of service obtained is still justified. Areas having large numbers of eDevices may wish to evaluate linking these users together under a single service contract for sharing a set amount of minutes per month.

H. Complaints regarding eDevices, service, or service contracts, should be filed with the USC Purchasing Department and/or the vendor.

I. All eDevice service contracts must be established in the name of the University of South Carolina. All eDevice service agreements must reflect the billing address of the local area or department paying for the device. In order to maintain full accountability at the user level and to eliminate establishing multiple purchase orders, it is strongly recommended that departments use their Visa Purchasing card to pay monthly bills for eDevices. Records of billing and payment should be maintained as required by University policy and procedure. Budgeting and tracking of cell phone charges must use the following object codes:

52037 – Cellular/wireless monthly charge
52038 – Cellular/wireless equipment and/or accessories

J. Personal eDevices may not be placed on state contract.

K. Service contracts for eDevices may be activated, cancelled, or service shifted to another vendor without cost to the University. Vendors should be notified in writing in advance of such a change. In the event that a personal eDevice must be used for conducting University business, the individual, with proper documentation of the personal air time used, may seek reimbursement.

L. Records indicating usage, monthly access and other charges are available under the Freedom of Information Act in University Policy UNIV 2.00 Freedom of Information Policy (http://www.sc.edu/policies/univ200.pdf) and are subject to audit. Therefore, users are strongly encouraged to use eDevices only for University business and to maintain accurate records.

M. A listing of cellular/wireless vendors, allowable charges and contracts authorized by the state may be found at the following web site: https://www.admin.sc.gov/sites/default/files/flipbook/ITSharedServicesCatalog/36/

RELATED UNIVERSITY, STATE AND FEDERAL POLICIES

UNIV 2.00 Freedom of Information Policy
UNIV 1.51 Data and Information Governance
UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
UNIV 1.60 HIPAA Compliance
UNIV 3.02 Enterprise Risk Management
IT 1.00 Information Technology Program Management

~~IT 3.00 Information Security~~

~~History of Revisions~~

~~Date of Revision~~	~~Reason for Revision~~
~~September 24, 2020~~	~~Policy reviewed and updated as appropriate.~~
~~September 8, 2010~~	~~Policy revised to reflect policy category change from IT 2.18 to BUSF 7.08. Policy organization, content and accuracy reviewed; no substantive revisions required.~~