UNIVERSITY OF Cincinnati	*Policy Title:* **Wireless Communication Stipend**	*Policy Number:* **2.1.7**
Category: Financial **Policy applicable for:** Faculty/Staff	**Effective Date:** 07/01/2014 **Prior Effective Dates:** 9/1/2011, 9/1/2008 **Enabling Act(s)** University Rule 10-5-04 IRS rule	**Policy Owner:** Sr. VP for Administration and Finance **Responsible Office(s):** Controller Payroll UCIT Office of Information Security

Background

This policy allows the University of Cincinnati to manage its business needs for wireless communication devices (including mobile phones, tablets and other devices with cellular/digital network capability) in a fiscally responsible manner while complying with federal regulations and UCIT Office of Information Security policies.

Policy

The University of Cincinnati may provide a wireless communication stipend to an employee who has a documented official university business need for a communication device. Organizational units may use the guidelines provided in this policy to determine whether an employee qualifies, based on the unit's needs.

The wireless communication stipend is intended to reimburse the employee for the business use of the device. The stipend is not intended to fund the cost of the device nor pay for the entire monthly bill. The assumption is that most employees also use their wireless communication devices for personal calls and/or data consumption.

Mobile phones, tablets, and other wireless devices should not be selected as an alternative to other means of communication, such as land lines, pagers and radio phones, when such alternatives would provide adequate and less costly service to the university.

The university does not reimburse, purchase or enter into mobile device or data contracts except as noted below in the section regarding university-owned devices.

Stipend Eligibility Guidelines

To qualify for the wireless communication stipend, the employee must have a business need, defined and approved by the supervisor. The following guidelines may be used as an organizational unit and the supervisor determine eligibility:

- The employee's job requires that they work regularly in the field and need to be immediately accessible.

- The employee's job requires that they need 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 and needs to be accessible or have access to information technology systems while traveling.
- Access via voice and/or access to information technology systems via a mobile communications device would, in the judgment of the supervisor, render the employee more productive and/or the service the employee provides more effective, and the cost of mobile communications service is therefore warranted.

This access may be limited to voice communications or also require access to information technology systems—e.g., email, calendar, Web, UC portal, etc.

Wireless Communication Stipends

The wireless communication stipend does not constitute an increase to base pay, nor will it be included in the calculation of percentage increases to base pay due to raises, job upgrades, retirement or other compensation increases. The stipend will be itemized on pay stubs, reported on employees' W-2s and subject to withholding taxes.

The monthly maximum stipend amount is established by the Office of the Controller and approved by the Vice President of Finance. See the Variant Expense Rate Table (see *Related Links*) for allowable stipend amounts.

The determination of the stipend amount covers the employee's projected business-related expenses only.

Responsibilities of Employees Receiving Stipend

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

- The employee will provide the phone number within five days of activation and will be available for calls (in possession of the wireless communication device and have it turned on) during those times specified by management.
- The employee may select any wireless carrier whose service meets the requirements of the job responsibilities as determined by the supervisor or organizational unit head.
- The employee must inform the university when the eligibility criteria are no longer met or when the wireless service has been cancelled.
- Management may periodically request that the employee provide a copy of the first page of the phone bill in order to verify that he/she has an active wireless

phone plan. Management may also periodically request documentation of substantial business use.

- The employee is responsible for all charges on his/her personal wireless plan, including early termination fees. If the employee leaves the position, he/she continues to be responsible for the contractual obligations of his/her wireless plan.
- The employee is personally responsible for complying with international, federal, state, and municipal laws regarding the use of wireless phones and other communication devices while driving. Under no circumstances will the University of Cincinnati be liable for non-compliance.
- The employee should use discretion in relaying restricted data (as defined per UC's Data Classification Policy) over wireless devices as certain wireless transmissions and/or devices may not meet the data security and/or compliance requirements for transferring or storing restricted data. See more on security for wireless communication devices below.

Data Security and Compliance

The university reserves the right to require any mobile device accessing the university's infrastructure to be subject to future mobile device security policies and guidelines as established by the university's Office of Information Security and IT governance structure. By connecting a wireless device to UC's network and/or utilizing it to access the university's systems and resources, UCIT is granted authorization to access and manage settings on the device for purposes of technical troubleshooting and performance monitoring. In select cases, UCIT Office of Information Security, under the guidance of the Office of General Counsel, may access wireless devices to perfom data breach or technology abuse investigations, and reset or wipe the device to mitigate the risk of exposing the university's data. This applies to both university and personally-owned devices.

Security policies may include device requirements for configuration, mobile anti-virus/spyware, mobile firewall, secure communications, encrypted file folders including storage cards or full device encryption, strong passwords, two-factor authentication, and/or destruction and disabling in the event of a lost or stolen device. Costs for any mobile security measures will become the financial responsibility of the organizational unit and/or the individual owner of the device at the time such requirements become university policy.

Wireless Communication Stipends on Sponsored Projects

Contact your grants administrator for guidelines and restrictions for charging wireless communication stipends on sponsored projects.

University-Owned Wireless Communication Devices

With the approval of the president, a senior vice president or a vice president, the university may purchase a wireless communication device with its associated plan in certain limited circumstances—e.g., phones or devices that rotate among student affairs, facilities or maintenance personnel. No personal calls are allowed on university-owned wireless communication devices. They should generally not be assigned to a specific individual nor taken home on a regular basis.

Upon approval of the president, a senior vice president or a vice president, the organizational unit may purchase a wireless communication device with its associated plan from any provider meeting the security requirements of the policy.

Miscellaneous

Extraordinary business use of an employee's personal wireless device in excess of the monthly stipend may be reimbursed with appropriate documentation and approval.

Exceptions to this policy require approval from the president, a senior vice president or a vice president.

Misuse or fraudulent receipt of a wireless communication stipend may result in progressive administrative and/or disciplinary action up to and including termination of employment and criminal prosecution.

Procedure

UC Flex GL Account	*535604* (Communications Stipend)

To initiate the electronic workflow process for a wireless communication stipend, the employee must submit a request through their supervisor. Supervisor must provide written approval of the stipend including the tier amount to the unit's business administrator, who will initiate a Personnel Compensation Request (PCR).

Wireless communication stipends will remain active until the employee and the organizational unit review the continued business need for the stipend and update any stipend amounts. At that time, the unit may require the employee to provide documentation of plan coverage and business use.

Organizational units may institute policies more, but not less, restrictive than this policy (2.1.7) if desired.

Related links:

IRS Guidelines
Policy Exception Form
Variant Expense Rate Table
Data Protection Policy
Network Connection Policy
Use of Information Technology
Password Policy
Mobile Privacy Policy
HIPAA Information Security Policy
Vulnerable Electronic Systems Policy

Phone Contacts:

Controller	556-3152
Grants Administrator	
Payroll Operations	556-2451
UCIT Office of Information Security	558-4732
Unit Business Administrator	