UWG PROCEDURE NUMBER: 8.2.5, Cellular Telecommunication
Authority: UWG POLICY: 8.2 Data Security Policy

The Chief Information Officer, pursuant to the authority of UWG Policy 8.2, establishes the following procedures on Cellular Telecommunication:

A. Definitions
   1. Approving Official – the department head. In the instance where the approving official is also the receipt of the device, the approving official is his/her supervisor.
   2. Department Head – the departmental authorized approver as identified and published by the Controller’s Office: http://www.westga.edu/controller/index_16157.php
   3. Usage Sensitive Services – those services whose recurring charges are based on a per unit measure such as minutes used, data transferred, or per occurrence of use. Examples include wireless Internet service, cellular airtime, text messaging, roaming charges or access fees for service outside of the USA, where such services are charged on a per minute or per occurrence basis.
   4. Wireless Communications Device (WCD) for purposes of this policy WCDs include devices that receive or send cellular data for the purpose of providing academic or business related data, voice, and text messaging communication services. Examples of such devices include, but are not limited to: wireless internet access devices (air cards or mifi’s), cellular phones, smart phones, and tablets.

B. Procedures
   General Guidelines
   It is the responsibility of UWG to implement procedures to effectively use communication services and equipment at the lowest possible cost. With the rapid growth in wireless communication devices used for both personal and business reasons, it is essential the University appropriately evaluate their applicability to support the academic mission and improve business operations.

1. Criteria for Determining Need
   A wireless communication device (WCD) and/or data service may be acquired for an employee where communications needs cannot be met with other available alternatives such as a radio or standard telephone equipment, and funding is available to support the acquisition. Examples of conditions under which a WCD and/or data service may be obtained include the following:

   a. A WCD/data service may be needed for employees whose job includes responsibility for protecting the physical safety of the general public and/or responding to environmental emergencies;
   b. A WCD/data service may be needed for employees who frequently need to communicate with students or access online resources while away from their desk or off campus;
c. A WCD/data service may be needed for on-call personnel required to respond to critical system failures or service disruptions;
d. A WCD/data service may be needed for additional protection for the employee in potentially hazardous working conditions and/or isolated areas;
e. A WCD/data service may be needed for an employee that is expected to do business while commuting and moving from appointment to appointment and/or has frequent travel;
f. A WCD/data service may be needed for an employee who cannot meet communications needs with other available alternatives.

2. Guidelines for Acquisition and Use
Specific University offices will assist in determining the necessity for a WCD and/or any associated data services:

a. The Department Head shall determine if a WCD and/or data service is necessary for a faculty or staff member to perform his or her duties, and select the appropriate airtime package based on that use (cellular minutes, texting, and data).
b. Each Department Head or his/her designee will maintain an inventory of the wireless devices the department has purchased. The inventory of WCDs shall document, at a minimum: the justification for necessity; each individual device type; applicable monthly charges, telephone number assigned, and the service provider for the device; the department contact number; the assigned user(s) (individual user or organizational unit in the case of shared/pool devices); and the authorized uses of the wireless or mobile device(s). Such inventory must be updated at least annually and made available for inspection by authorized offices or agencies.
c. Each Department Head or his/her designee will periodically review the use of departmental WCDs to ensure the use plan is still cost effective and no excessive charges are being incurred. Such review should occur no less than once per semester, and documentation of the review shall be maintained in the department.
d. The individual to whom a WCD is assigned is responsible for safeguarding the equipment and controlling its use. Transmission and storage of data on the WCD must follow the existing security guidelines and UWG's current Acceptable Use Policy. See the Additional Resources section for more information. Employees are expected to avoid the use of the equipment under any circumstances where such use might create or appear to create a hazard. Lost or stolen devices should be reported to the department head as quickly as possible prevent unauthorized use.
e. Individual users of a WCD should limit personal use of the device, and are responsible for reimbursing the University in the event that personal use results in additional charges to the University.
f. Upon discontinuation of use of a WCD, the equipment should be collected by the Department Head and promptly forwarded to Information Technology Services for disposal.
g. A University account (@westga.edu) must be used to manage applications and data on a University owned device.

To the extent any of the provisions set forth in this procedure are in conflict with state law, the latter will control.
Ordering Cellular Telephones and Associated Service
All orders for cellular telecommunication products or services must follow the procedures established by the UWG Purchasing Office.

Right to Monitor Communications and Open Records
The University reserves the right to investigate, retrieve, and read any communication or data composed, transmitted, or received through voice services, online connections and/or stored on its servers and/or property, without notice to employees. This includes any personal information that may be stored or available on the wireless device.

C. Compliance
Failure to comply with this policy may result in disciplinary actions under applicable UWG and State policies, procedures, and laws.

Issued by the Chief Information Officer, the 12 day of April, 2019.

Signature, Chief Information Officer

Reviewed by President:

Previous versions:
-July 31, 2017
-2008 (converted to new format 2013)