

# STOCKTON UNIVERSITY



## PROCEDURE

### **Mobile Devices and Commercial Wireless Network Service**

Procedure Administrator: Chief Information Officer and Chief Financial Officer

Authority:

Effective Date: December 16, 2009; September 26, 2012; October 31, 2019

Index Cross-References: Procedure 4200 - Acceptable Usage Standards of Computing and Communication Technology

Procedure File Number: 6420

Approved By: Harvey Kesselman, President

“Mobile Device” means any mobile communication device issued by the University to employees for business use including, but not limited to, smartphones, cellphones, tablets, notebooks, hotspots and other similar devices.

Employees are required to use Mobile Devices in accordance with the procedures established herein, University Procedure 4200, and all other applicable University policies and procedures.

Mobile Devices are not the private property of the employee. Mobile Devices, and the statements, summaries, and files related to Mobile Devices, are property of the University, which in certain circumstances may be subject to public disclosure in accordance with University policies and procedures, and as required by law.

If an employee uses a Mobile Device in violation of University policies or procedures, the University may restrict or terminate the employee’s access to the Mobile Device and the employee may be subject to disciplinary or administrative action, as appropriate, up to and including termination from Stockton University and, where appropriate, civil and/or criminal liability.

### **Mobile Device User Responsibilities**

Employees are responsible for the use and access of all Mobile Devices. All Mobile Devices shall be used only by the employee to whom it was issued. The employee is responsible for securing the Mobile Device with a password or PIN. Employees are responsible for all activity on the Mobile Device, and are expected to take appropriate safeguards to ensure that the Mobile Device’s password or PIN and all information and data on the Mobile Device are private and not disclosed to others. Employees also shall not provide unauthorized users access to the accounts, computing or communication system, or data on the Mobile Device.

Excess personal usage of any Mobile Device will be determined by the supervisor of the employee or University administration, and may be monitored per University policy and procedures. Employees may be required to reimburse the University for any personal use of a

Mobile Device that results in excessive toll or usage charges to the University. Users of University Mobile Devices may be responsible for the repair or replacement of a damaged, lost, or stolen Mobile Device, if such damage, loss or theft was due to the employee's negligence. Employees are responsible for promptly returning all Mobile Devices to the University when the Mobile Device is no longer required to carry out the employee's job responsibilities, or upon termination of employment.

Employees may use Mobile Devices for email, communication, and other tasks as required by the University. Employees may install University-approved software or applications on Mobile Devices as necessary or required in the performance of the employee's job responsibilities.

### **Mobile Devices and Commercial Wireless Network Service**

Mobile Devices will be issued by the University to employees based on their job responsibilities. Mobile devices and commercial wireless network service may be provided in cases where the performance of the employee's job responsibilities routinely requires access to services or communications using a tablet, notebook or similar Mobile Device during times when the employee is out of the office and cannot use a secure cost-free alternative, such as secure Wi-Fi or wired access.

The purchase of all Mobile Devices, and the connection to and use of any commercial wireless network service, will be coordinated through Information Technology Services.

The use of Mobile Devices and associated commercial wireless network services must be approved by the appropriate divisional cabinet member. This approval will be determined based on job responsibilities, eligibility for commercial wireless network service, and the needs of the University. The University reserves the right to revoke the use of a Mobile Device and commercial wireless network service at any time for any reason, or for no reason. If an employee changes positions within the University, the employee's new divisional cabinet member will determine whether the employee has a continuing need for a Mobile Device and connection to commercial wireless network service. The employee's supervisor will discuss expectations on the availability of the employee and use of the Mobile Device before issuing the Mobile Device to the employee.

### **Eligibility for Commercial Wireless Network Service**

Mobile Devices with commercial wireless network service may be issued to employees who meet specific job-based eligibility criteria and have approval of their divisional cabinet member. Factors that will be considered for different divisions include, but are not limited to, the following:

Information Technology: Employees who are required for emergent responsibilities, after-hours support, or additional communication needs regarding emergency technical services and support.

Facilities/Plant: Employees who are required for emergent responsibilities, are always in the field, or do not have regular access to a landline phone.

University Relations and Marketing: Employees who must be available for media and community relations, crisis management, or additional communication responsibilities regarding the University's public image.

Emergency Management and Campus Public Safety: Employees who must be available to respond to emergencies regarding the safety of the University community, or additional communication needs regarding emergency services.

Development: Employees who are required to remain in contact with both the office and donors. These employees are responsible for obtaining donations from corporations and other entities.

Student Affairs: Employees who must be available for situations dealing with the welfare of University students.

Management: Senior level or executive management that directly support presidential initiatives and communication efforts, as well as oversee administrative, managerial, and operational functions.

For purposes of this Procedure, an “emergent situation” arises when, in the discretion of the University, there is an important need for timely contact with an employee. In limited circumstances, employees who do not consistently meet the criteria above may be issued a University-owned device for when such criteria are met. This includes: (A) When the employee’s job function requires considerable time outside of their assigned office or work area; (B) When it is important to the University that they are accessible during those times; and (C) When the employee’s job function requires them to be accessible outside of scheduled or normal working hours.

## **Reimbursement for Use of Personal Commercial Wireless Network Service Plan**

### **Full Authorization:**

The University, through the appropriate divisional cabinet member, may authorize reimbursement for a commercial wireless network service plan for an employee who uses a personal mobile device for University business. The University will not reimburse employees for the cost of the personal mobile device. The University will consider the following criteria to authorize a reimbursement: (A) Whether the employee’s job responsibilities requires significant time outside of the employee’s assigned office or work area; (B) Whether the employee must be accessible to the University when the employee is outside the assigned office or work area; and, (C) Whether the employee’s job responsibilities require the employee to be accessible outside of scheduled or normal working hours.

If authorized, the University will reimburse the employee for commercial wireless network service for the lesser of (i) \$45 per month or (ii) the actual cost of the employee’s individual line of service. If the employee’s plan has multiple lines of service, the reimbursement will be based off the average cost per line on the employee’s service plan. To receive reimbursement, the employee is responsible for submitting to the University, at least quarterly, the bills for their commercial wireless network service plan. Under no circumstances shall the approved reimbursement amount exceed the actual charges for the employee’s individual line of service.

### Limited Authorization:

Employees who have not received full authorization for reimbursement of commercial wireless network service under this procedure will not be reimbursed for the use of their personal cellular device unless otherwise approved by the appropriate divisional cabinet member for limited purposes and for a limited time for business usage. Any limited authorization will be considered on a case-by-case basis.

### Recordkeeping and Review

Each Budget Unit Manager is required by the University to review, at least quarterly, usage statements for all Mobile Devices and any reimbursements for use of personal commercial wireless network service plans within their budget unit. At the discretion of the University, employees may be required to reimburse the University for any personal use of a Mobile Device that results in excessive toll or usage charges to the University.

If an employee plans to use a Mobile Device during international travel, the employee must provide written notice at least ten (10) business days prior to departure to the appropriate divisional cabinet member and Information Technology Services. The University will audit Mobile Devices for international usage and employees may need to reimburse the University for excessive personal use of Mobile Devices during international travel.

Information Technology Services will conduct a regular review of Mobile Devices and commercial wireless network services and coordinate, as necessary, with Budget Unit Managers to ensure appropriate assignment and use of such devices and services.

### Review History:

	Date
Chief Information Officer	8/31/2019
General Counsel	9/27/2019
Cabinet	10/31/2019
President	11/04/2019