PURPOSE

This AP outlines a set of practices and minimum requirements for the safe use and management of College-issued mobile devices. This AP applies to all College-issued mobile devices, including the devices already in use by authorized College employees.

SECTION 1: DEFINITIONS

1.1 “AP” means Administrative Procedure.
1.2 “Mobile devices” include removable storage devices (e.g., USB flash drives, external hard drives), portable communications and computing devices (e.g., laptops, notebooks, tablets, PDAs, telephones) and other similar devices.

SECTION 2: PROCEDURE AND RESPONSIBILITIES

2.1 Acceptable Use of College-Issued Mobile Devices

College-issued mobile devices are intended to be used solely for official College work-related purposes, including: a) as the primary computing device on campus; b) as the primary or alternative device while traveling on official College business; c) any other College work-related tasks.

Incidental use of the College-issued devices by the employee is permitted for personal use, provided that such use is otherwise consistent with this AP. However, employees may be required to reimburse the College for any usage resulting in unauthorized charges.

College-issued mobile devices should not be used by anyone other than the College employee to whom the device was issued.

2.2 Privacy Expectations

College employees do not have a right, nor should they have an expectation, of privacy while using College-issued mobile devices at any time, including accessing the Internet and using e-mail and voice communications. By acceptance of the College-issued mobile device, employees consent to disclosure and/or monitoring of device usage, including the contents of any files or information maintained or passed-through that device.

2.3 Responsibilities of Employees

Each employee is responsible for the safekeeping and care of the assigned mobile device.

If the College-issued mobile device is damaged, lost or stolen, the employee must immediately report it to the issuing department.

Upon resignation, retirement, or separation from the College, the employee must return all College-issued mobile devices and all accompanying accessories to the issuing department on or before the final day of work. Failure to timely return
College-issued mobile device will result in College's withholding from the employee's final paycheck the costs of device replacement and any costs associated with collection of the device from the employee.

2.4 Security

All College-issued mobile devices must be enrolled into the College's mobile device management program at all times.

All College-issued mobile devices that access or store sensitive, confidential, or personally-identifiable information must be encrypted.

All College-issued mobile devices, where possible, must be secured using a PIN or other password protection.

All College-issued mobile devices must be kept up to date with the latest security patches, virus-scanning software and virus data files, and firewalls.

All College-issued mobile devices, where possible, must have remote data wipe capability installed and enabled. The data will be wiped from the mobile devices, either directly or remotely, in the following circumstances:

a. Whenever the mobile device is reported lost or stolen
b. After 10 failed password attempts
c. Whenever the College IT detects a data breach, a virus or similar threat to the security of the College data and technology infrastructure
d. Before transferring possession of a mobile device from one College employee to another
e. Before disposing of the mobile device

The security protections for College-issued mobile devices will be reviewed at least annually.

2.5 Enforcement

Non-compliance with this AP may result in disciplinary action and/or revocation of College-issued mobile devices.

2.6 Authority
The Vice Chancellor for Information Technology is responsible for implementing and overseeing compliance with this AP.

Before issuing a mobile device to an employee, the Vice Chancellor for Information Technology or designee shall require the employee to sign an Employee Mobile Device Agreement. The Vice Chancellor for Information Technology or designee shall maintain a record of all Employee Mobile Device Agreements.

SECTION 3: EMPLOYEE MOBILE DEVICE AGREEMENT

EMPLOYEE MOBILE DEVICE AGREEMENT

[NOTE: A new Mobile Device Agreement must be completed for each device issued].

By accepting the College-issued mobile device (“Device”), [Employee name]__________________ (“Employee”) agrees to the following terms and conditions:

1. Authorized Use

a. Employee shall use the Device for College work-related purposes. Occasional personal use is permitted, provided that Employee otherwise complies with the terms of this Agreement.

b. Employee shall be the sole authorized user of the Device and shall not share the Device with others.

c. Employee shall, at all times, comply with the College's Acceptable Use of Information Technology Resources policy.

d. Employee acknowledges that the employee does not have a right of privacy while using the Device at any time. College may monitor and require disclosure of device usage, including the contents of any files or information maintained or passed-through the Device.

2. Security and Employee Responsibilities

a. Employee shall comply with all mobile device security guidelines required by AP-9.01.XX, College-Issued Mobile Device Security, as implemented by the College IT Department.
b. Employee shall be responsible for the safekeeping and care of the assigned Device.

c. In the event the Device is damaged, lost or stolen, Employee shall report it to the College IT Department within 24 hours.

d. Employee acknowledges that in the event the Device is lost or stolen, the College IT Department may remotely wipe all data from the Device. Employee shall be solely responsible for loss of any personal data stored on the Device.

e. Employee shall, upon resignation, retirement, or separation from the College, return the Device and all accompanying accessories to the College IT Department on or before the final day of work. Employee understands that failure to timely return the Device may result in withholding the costs of device replacement and other costs, including attorneys' fees, from Employee’s final paycheck.

By signing below, I understand and agree with the terms and conditions of this Agreement:

Employee Name

Job Title  Campus/Department

Date  Signature

Purpose

The purpose of this AP is to establish minimum standards for the protection of College-owned portable computing devices and the data that resides on them.

Definitions

A. Portable computing devices, such as laptops, notebooks, tablets, PDAs, telephones and other handheld devices are vulnerable to damage, theft or loss by nature of their portability. Each device, as well as the data stored on or accessed by the device, needs to be secured in order to protect confidential and sensitive information that is often stored on it.

B. Physical security denotes safeguarding the portable device itself from theft or from physical damage caused by falls, abuse of electrical cords, exposure to liquids or food particles, exposure to particulates, overheating, electrical spikes, and proximity to strong magnetic fields.
C.—Data security denotes safeguarding from unauthorized access all data and software residing on the portable device, as well as any on the College network to which the device may connect. This includes but is not limited to: College email, the College Intranet, data files, and commercial software.

D.—Data security methods involve password protection, encryption, keeping the device within the employee’s physical proximity at all times, and other means.

Procedures and Responsibilities

A.—Users must secure portable computing devices from unauthorized physical and data access. Specific strategies for physically securing portable devices include but are not limited to: never leaving a device unattended in a public setting; transporting them as carry-on luggage whenever possible while traveling; keeping them covered or otherwise out of sight while locked in vehicles; using cables to secure the device to a desk whenever possible.

B.—All portable computing devices should be kept up to date with the latest security patches, virus-scanning software and virus data files, and firewalls.

C.—Encryption methods will be used on all business-critical or sensitive information related to the College. The portable device should contain only that College data needed during travel. Power-on passwords should always be enabled when possible. The display screen should be locked and the device physically-secured by cable if it is to be left unattended even for brief periods of time.

D.—Theft or loss of a portable computing device must be immediately reported to the local authorities, department supervisor and the IT department from which the equipment was obtained.