POLICY TITLE: MOBILE COMPUTING DEVICE POLICY

I. Purpose

The purpose of this policy is to set out the permitted manner of use of mobile devices on the College's network by its employees, students, guests and contractors, and the use of College-issued mobile devices in any environment in order to maintain the security and integrity of the College's network and data infrastructure, and maintain the confidentiality of College data which may be accessed or placed on mobile devices.

II. Scope

This policy applies to any mobile device (College-issued and personal) that can access the College's network via wired or wireless connections.

III. General

A. Definitions

1. Mobile device
   A mobile device is any device that combines telecommunication and computer functions and is easily carried on a person. Examples include, but are not limited to, laptop computers, "smart phones" (e.g., RIM Blackberry, Apple, Android, etc.) and "tablets" (e.g., Apple iPad, Amazon Kindle, etc.).

2. College-issued mobile device
   A College-issued mobile device is any mobile device owned by the College and distributed by the College's Information Technology Services (ITS) Division. ITS will maintain administrative control of such devices including remote lock and remote wipe functions, which may be used in the event the device is lost or stolen or its security is otherwise compromised.

3. Personal mobile device
   A personal mobile device is any mobile device that is not a College-issued mobile device.

4. Encryption
   Encryption means using electronic and physical methods to make clear text information unreadable to unauthorized persons.

B. College-Issued Mobile Devices

College-issued mobile devices may use the College's network and network services as needed to perform the College's business and for other College-approved tasks. A signed and approved "Employee Mobile Device User Agreement" is required before a mobile device will be issued to a user.

Users of College-issued mobile devices may use the device for normal personal use like email, social networking and web browsing, subject to limitations contained in this and other College policies. Excessive personal use or careless actions that lead to the compromise of the device may result revocation of use privileges and/or disciplinary actions.

Each user is responsible for ensuring that the College-issued mobile device is used only in compliance with the Acceptable Use Policy and College guidance on security procedures, safe user behaviors, etc. The user is responsible for ensuring that personal use does not expose a College-issued mobile device to malware, malicious web sites, or other security risks.

Each user is responsible for the physical security of the College-issued device assigned to them and must immediately report any theft, loss, damage, or vandalism of the unit to the LCC ITS Help Desk. Immediate notice concerning a lost or stolen mobile device is critical, so that unauthorized and/or inappropriate access can be minimized. The assigned user is responsible for any unauthorized and/or inappropriate access to College information that occurs from the misuse, loss or theft of mobile devices.

The College may, at its discretion, change the method by which a device connects to the network and change the configuration of the device, without the user's consent or knowledge, to prevent unauthorized use or access to College data. These configuration changes include, but are not limited to, upgrades to the device's operating system and software, locking the device to prevent use, changing the device's access code, and the deletion of all data/files on the device.

Users of College-issued mobile devices are prohibited from storing information on the device in ways that may violate laws and regulations regarding the security or privacy of health records, student records, credit card and loan information, etc. Accessing such information is prohibited unless accomplished via a secure and encrypted means if the device is not directly connected to the College's network. Also, users are prohibited from using such devices to violate copyrights including, but not limited to, copyrighted music, movies, software and publications.

The College uses technologies such as encryption, identity management, anti-malware, anti-virus, and remote administration to protect all of the mobile device's data whether that data is at rest, in use, in transit or being destroyed.

C. Personal Mobile Devices

The College maintains networks that are based on available business services. Personal mobile devices are normally limited to using a guest network that will provide access only to Internet and printing services. Use of personal mobile devices to access any other College network is permitted only with the written approval of the Director of Information Security. Such approval must be requested in writing, and will be granted only if the user enters a written agreement authorizing the ITS Division to install and maintain software (e.g., remote administration, encryption, etc.) deemed sufficient to meet College standards for security and control. Users of personal mobile devices must comply with all standards that apply to the use of College-issues mobile devices.

D. Contractors

Contractor owned equipment will be treated as personal mobile devices. LCC sponsors of contractors are responsible for communicating this policy to them. The Director of Information Security may waive application of portions of this policy to a contractor if the Director determines such waiver is necessary and appropriate to facilitate the completion of any project under the direction and control of the College and under the supervision of College personnel. Such a waiver must be in writing.

E. Mobile Usage of Mobile Devices

The use of any mobile device in violation of applicable law or regulation is prohibited. The use of any mobile device other than a hands-free cell phone is prohibited while the user is operating a motor vehicle on College business. The use of any College-issued mobile device other than a hands-free cell phone is prohibited while the user is operating a motor vehicle, whether or not on College business. LCC strongly recommends against use of any mobile device while operating any motor vehicle under any circumstances. Drivers must use their judgment regarding the urgency of the situation and the necessity to use a cell phone while driving, but should generally make every effort to move to a safe place off of the road before using a cell phone.

IV. Responsibility

The Director of Information Security is responsible for educating staff, faculty, students, guests and contractors regarding this policy. The Director of Information Security is responsible for preparing procedures and instructional materials to implement this policy. The Director of Information Security is responsible to report to the Chief Information Officer on the effectiveness of this policy in regards to information security using appropriate metrics.

Any question of interpretation or application of this policy shall be referred to the Chief Information Officer (or designee) for final determination.

This policy shall be reviewed every year under the direction of the Chief Information Officer (or designee).

Adopted: 12/17/12