MOBILE COMMUNICATION DEVICES PROCEDURE

Related Board of Trustees Policy: BP 8.4
Approval: August 2012
Revision:
NC Statewide Technology Standards: 050406 and 50710

Purpose: NC Statewide Information Technology Standard 50406 requires all college sponsored mobile technology users must be informed of the following guidelines to help safeguard confidential information while using Craven Community College provided cell phones/tablets. Protect state resources and confidential information during mobile communication device use.

A **Mobile Technology Use Form** will need to be completed and signed by the College employee.
All mobile devices will be requested through the college Technology Services department via the college help desk system. For purposes of this procedure "mobile communication devices" includes, but is not limited to, mobile phones, IP phones, pagers, BlackBerry devices, iPhones, and smart phones. Some of these devices are multifunctional and may be used for voice calls, text messages, e-mail, Internet access, and may allow access to computers and/or networks.

Any personal use of a cell phone, smartphone, netbook or other device for which the college is charged a fee must be reimbursed by the employee incurring that charge. Each employee assigned a mobile communication device will be required to read, understand, and sign the **Mobile Technology Use Form.**

An individual should turn in all mobile devices to the Technology Services department if he/she is no longer employed by the college, if the device is broken and needs repair/exchange, or if the device is to be upgraded.

The Technology Services department is responsible for:

- Ordering the mobile device through the appropriate provider.
- Setting up access to the college e-mail system on the mobile device. All security measures will be applied during this set up process.
- Resetting the mobile device back to factory defaults when it is turned in due to obsolescence, not being in working order, or if the individual user is no longer employed by the college.
- Removing all data before disposing of the device.

In order to protect mobile communication devices used to conduct college business, the following measures are communicated to individual receiving a college issued device:

- Use a password that follows password policy standards to protect the device.
- Do not open attachments from untrusted sources.
- Do not follow links from untrusted sources, especially from unsolicited e-mail or text messages.
- Adhere to state and college policy when downloading software.
- Report lost devices immediately to the Technology Services department. Use the remote erase function if enabled.
- Review the mobile device security settings to ensure appropriate protection.

Return to the Table of Contents