CPTC Procedure: Mobile Device Procedures

Coastal Pines Technical College (CPTC) provides mobile devices to employees to support the effective performance of their jobs. These mobile devices are primarily intended for business purposes. Each individual who requests or is assigned a mobile device is responsible for safeguarding the equipment and controlling its use. ***Note: this procedure is a derivative of a section of the TCSG Security Guidelines. Any changes or differences in the TCSG document will supersede the CPTC procedure.***

Guidelines:

Several guidelines should govern employee usage of college-issued mobile devices.

1. Any employee assigned the use of a cellular device is expected to exercise discretion regarding persons having access to the employee's cellular phone number in an effort to minimize phone usage costs while maintaining departmental service capabilities.
2. Cellular phones, mobile devices, and air cards are not to be used when a less costly alternative such as an office phone or Wi-Fi is readily available. (When charges apply.)
3. Employees using a college-issued cellular phone are not permitted to withhold their cellular phone number from other employees who need it to conduct business.
4. The College will provide one data-enabled device to users that have multiple mobile devices. Exceptions are on a case by case basis with approval by the College President being required. (Tethering on college cell phones can add data capabilities to other devices such as tablets and laptops by enabling a mobile hotspot on a cellular device. This costs approximately $10 additionally per month. This amount is subject to change, and it may not apply to all devices.)

Eligibility:

Employee eligibility to be assigned mobile devices under this policy will be defined as employees at the Cabinet level or:

- Employees whose primary job duties are performed outside of an office environment.
- Employees required to be accessible 24 hours a day, 7 days per week for emergencies.
- Employees who must work at multiple locations while being continually available.
- Other critical contacts (security, IT staff and key facilities staff).
- Department heads must document an employees' eligibility/need based on these requirements on a Cell Phone Request Form.
- Justification of need must be specific as to why other means of communication provided by the College (i.e. office phones, e-mail, etc.) are not adequate to meet the communication requirements of the employee's job.
- A Cell Phone Request Form must be completed and signed by the department VP/Executive Director and the Executive Director of IT and submitted to the Business Office.

Equipment:

Employees are limited to which mobile devices they may choose from.

- Data cell phones: Coastal Pines Technical College has standardized to the iPhone platform. If the need for mobile e-mail is identified and approved, all CPTC smartphones will be iPhone models chosen by IT. Existing phones may be used until they are phased out.
- All cellular devices are purchased through T-Mobile or other suitable vendor.

- The standard tablet is either an iPad or a Microsoft Surface Pro. Users may also select an Android-based tablet with a business case.
- Exceptions to these rules may be approved by the College President when a need arises.

Data Security:

Any mobile device used for business communications must be password, pattern, or PIN protected at all times when not in use. The PIN should be a minimum of 6 characters where supported. The device must be configured so that if the password, pattern, or PIN is incorrectly entered ten times the device must reset to factory defaults. *Note: this means that **all** data will be erased from the device.*

Employees must understand that any device (personal or college-issued) used for business communications is subject to remote wipe of all contents by the College Information Security Administrator (ISA) or TCSG ISO if there is a potential security issue. (CPTC's ISA is the Executive Director of Information Technology.)

Employees are responsible for securing their devices to prevent non-public data from being lost or compromised. Information not intended for public dissemination should never be transmitted. Further, employees may be held responsible for the consequences of a data breach. (See the ***CPTC Procedure: Mobile Computing and Removable Storage Device Procedure*** and ***CPTC Procedure: Use of Personal Mobile Devices (PMD) for Business Communications*** for more information.)

Appropriate Use:

CPTC cell phones and cellular service are purchased to be used as a business tool.

1. The primary use of e-mail, texting, and calls should directly relate to official college business with personal use being brief and infrequent.
2. CPTC cell phones should not be used to call directory assistance services such as "411" except where unavoidable.
3. Employees are responsible for promptly reimbursing the College for all non-business cellular device charges incurred.
4. The College also acknowledges that some mobile devices are capable of making on-line purchases from retailers. The College will not reimburse the cost of these purchases, and if purchases are applied to the monthly invoice, the employee will reimburse the College.
5. These voice and data services are not meant to replace an employee's home Internet or phone services. Overuse of data may result in rate-limited connection speeds.
6. Adding a mobile hotspot to enable data tethering has to be approved by both the division VP or Executive Director as well as the college president. Ideally, it should be approved sparingly.

Damage, Loss or Theft:

Employees should make reasonable precautions to prevent loss, damage, theft or vandalism to college-issued mobile devices.

1. The College will accept responsibility for equipment that is damaged in the course of business unless the damage is the result of reckless or deliberately destructive actions of the employee.
2. Equipment that is lost, stolen or damaged outside the course of business is the responsibility of the employee that the device is assigned to. The IT Department will

provide pricing information for the cost of a replacement device. The CPTC President may waive replacement costs.

3. All lost, stolen or damaged equipment should be brought to the attention of the employee's supervisor and the College ISA. For CPTC, the College ISA is the Executive Director of Information Technology. The supervisor or employee will contact the IT Department, and CPTC IT will contact the vendor for replacement or repair. Employees and supervisors are NOT to contact the cellular provider directly.
4. Lost or stolen equipment should be reported to the ISA immediately so the service can be suspended or cancelled, and the device can be remote wiped of contents if needed.

Safe Use:

In the interest of safety, employees using mobile devices are expected to exercise appropriate care and caution if used in a moving motor vehicle.

- Utilize hands-free technology when possible. The College does not provide hands-free technology except when state vehicles are Bluetooth equipped.
- Texting is strictly prohibited while driving.

Personal Devices:

Coastal Pines Technical College will not reimburse employees for business calls or Internet usage made on non-college devices. An employee who wants to request a College-issued cellular phone or College-provided mobile internet service should carefully review the eligibility requirements contained in this procedure before consulting with his/her supervisor or VP/Executive Director.

- Personal mobile devices can be utilized if the employee is willing to fund and support the device as long as they comply with all CPTC policies and procedures.
- If a personal mobile device is configured to retrieve employee e-mail, the employee acknowledges that college policy requires that any computer/device connected to the network is subject to the "State of Georgia Open Records Act." (This means that during a security audit or FOIA request, a list of remote users could be requested, and if deemed that those users connected to State resources from non-state devices that the equipment could be susceptible to search and/or seizure.)
- College e-mail, data and other business related communications are the property of the College regardless of where they are stored, and the mobile devices used for business communications are subject to search and/or seizure at any time, and there is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on the device used for business communications.
- For more information, see the ***CPTC Procedure: Use of Personal Mobile Devices (PMD) for Business Communications*.**

Usage Monitoring:

Identical to CPTC e-mail and other information stored on CPTC computers, all use is subject to review at any time. Cellular invoices may be audited on a monthly basis (or such other periods as the College may direct to examine usage). The College has the right to terminate and/or suspend or alter plans at any time. Employees will be made aware of overages or other incurred charges outside of normal billing.

Normal billing includes:

- Allocated talk time minutes (for most plans, this is unlimited)
- Limited data plan (depends on device), and in some instances, unlimited data
- Messaging Services: SMS & MMS

Not included:

- Tethering of devices for Internet services. There is a separate charge for enabling a mobile hotspot.

Responsibility

The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented.

Adopted: January 16, 2014
Revised: September 19, 2023