CPTC Procedure: Use of Personal Mobile Devices (PMD) for Business Communications

Definition of Personal Mobile Devices (PMD): Any portable electronic device capable of sending and receiving e-mail and/or accessing business data via wireless or cellular connection. The most common examples of this would be cellular phones and connected tablets.

Definition of Business Communications: Any e-mail, data or other communications transmitted to or from CPTC's systems. Also includes any other business-related communications regardless of source, destination or technology.

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.

1. Coastal Pines Technical College (CPTC) will use Mobile Device Management (MDM) software to encrypt and manage remote device e-mail and data services for all PMD users where possible. The selected product is Microsoft's Office 365 cloud email service. The product will be required to meet all TCSG security requirements while keeping corporate mail separate from the user's personal data and allows selective application of security policy to business applications and data only.
2. Business e-mail, data and other communications are the property of CPTC regardless of where they are stored.
3. Any personal mobile device used for business communications is subject to search and/or seizure in the event of a legal requirement for such.
4. There is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on a PMD used for business communications.
5. Any CPTC or personal mobile device used for business communications is subject to remote wipe of all device contents in case of loss, theft, or if the business data contained therein is considered at risk.
6. CPTC personnel 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 via PMD.
7. Any personal mobile device used for business communications must be password, pattern or PIN protected at all times when not in use.
8. If supported by the device, when the password, pattern or PIN is incorrectly entered ten times the device must reset to factory defaults (all data erased).
9. If supported by the device, encryption must be enabled.
10. CPTC personnel must abide by all municipal, state and federal laws pertaining to the use of personal mobile devices.
11. CPTC personnel using a PMD for business communications must sign and submit the Personal Mobile Device for Business Communications Terms of Use agreement when saving any business communications to a PMD.
12. Loss or theft of a PMD used for business communications must immediately be reported to your Information Security Officer or Administrator. The ISO/ISA or their designee will assist the user in remotely wiping their device using appropriate software or management applications such as Android Lost, JAMF, or Meraki MDM. If the device cannot be remotely wiped the user must immediately notify their carrier and request that the device be wiped clean and disabled.

13. All CPTC employees that use PMDs for business communications, CPTC-owned or personal, must agree to and sign either TCSG's PMD for Business Communications Terms of Use document (ISG-06a.1) or CPTC's version on the Intranet under forms → IT. This form will be stored as long as the employee uses a PMD for business communications for CPTC.
14. These guidelines will be revised based on changing information security requirements.

Responsibility

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

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