Title: Computers and Telecommunications	**Number:** 3.7	Page **1** of **4**
	Related Procedure? ☒ **Yes** ☐ **No**	
Legal Citation (if Applicable)	**Board Approval/Revision**: 26 March 2014	

1. Purpose
The purpose of this policy is to ensure the proper use of the Colorado Mountain College (CMC) computer and telecommunications resources and services by its employees, contractors, and other associates. All systems users have the overall responsibility to use the computer and telecommunications systems in an ethical, efficient, and lawful manner.

The rules and conditions outlined here, and in administrative procedures, apply to all users of all systems throughout the District and any other locations of CMC. Willful and intentional violations of the following policies may result in disciplinary action up to and including termination and necessary legal action.

2. College Support
The College supplies and supports only one computer device per employee exclusive of a cell phone. A computer device is defined as desktop computer, laptop computer, or other computer device necessary to perform the employee's job within his or her department.

3. Procedure
Information Technology (IT) annually sets a standard for both desktop and laptop computers. Standard computers are issued to all employees unless an exception is approved.

If an exception is requested, the model of the computer device is determined and approved by IT working in conjunction with the requesting department supervisor.

Exceptions to the policy may be granted in certain circumstances. Examples may include:

1. IT technicians and technical services staff are exempt from this policy because they need to support and service many different computer devices to perform their jobs.

2. Specific departments are exempt from this policy because the employees in these departments need additional devices to perform their jobs. For example, the Physical Plant Department has laptops placed in electrical and HVAC rooms so they can manage these systems.

3. Specific academic departments have mobile devices to use in the field that are checked out by faculty within the department.

It is the employee's and supervisor's responsibility to understand the functions and limitations of the device chosen. Device replacement follows the standard computer replacement cycle. This replacement cycle is determined by Information Technology Committee and approved by the Board of Trustees.

Supervisor approval is required for any non-standard device due to potential future impact to the department. If an employee chooses a computer device other than a desktop computer or a laptop, and

the employee leaves his or her position, the device shall not be replaced for a new employee's preference until the standard computer replacement cycle.

All computer devices are purchased through the IT Department.

4. Funding

Computer devices for full-time employees are included in the regular budget process through the annual computer replacement cycle.

Computer devices for part-time employees are funded by individual departments or campuses. For any device costing more than the standard computer, the department or campus is responsible for covering the difference in cost.

5. Mandatory Use

The College has the right to monitor any and all aspects of its computer and telecommunications systems including employee email, voice mail, and file structures on any CMC system. CMC's right to monitor its computer system and telecommunications equipment includes, but is not limited to, monitoring sites that users visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users, and reviewing email sent and received by users. All systems owned by CMC are intended to be used for CMC business purposes only. The computer and telecommunication systems are provided to the employees to assist them in meeting the requirements for the performance of their positions in CMC. However, while occasional and incidental personal use is acceptable, employees should not have an expectation of privacy in anything that they create, send, or intentionally receive on CMC systems. Since systems are provided for CMC business, transactions and data on the systems are considered to be business-related and therefore owned by CMC except when superseded by the College's policy on Intellectual Property.

Approval to monitor computer or telecommunications use must be given by the College President.

6. Confidential Information

All employees and those given access to CMC's technology resources have an obligation (and are required by law) to keep confidential all information obtained from others, including student information (as per FERPA Guidelines). Any questions regarding what information is public and available for sharing should be referred to an employee's immediate supervisor and/or the appropriate functional area. The confidentiality obligation also pertains to any party accessing any communication system.

7. User IDs and Passwords

All employees accessing any CMC computer or telecommunication system must have a unique User ID and password. This includes user accounts for the Local Area Network (LAN), servers, and task-specific software applications such as student or financial systems. To maintain system security, users are not to log in as another user. Generic logins are not issued unless an application, such as Colleague Software or a third-party system, requires it and no other viable solution is possible.

To protect themselves and the confidentiality of data, users are prohibited from disclosing their passwords to others. Logins and passwords are not to be written down and/or displayed or kept in places such as desk drawers, keyboard trays, etc. If a user suspects a password has been disclosed, the user is required to change the password immediately. User accounts are not transferable to temporary employees.

8. Software

All users must comply with all software licenses, copyrights, and all other state and federal laws governing software licensing and intellectual property. Violation of software license agreements is grounds for disciplinary action, up to and including termination.

The College President shall develop procedures to implement this policy.

9. Internet and Email

Users may be granted access to the Internet for informational and business purposes. The use of the Internet and email at CMC is a privilege, not a right. Inappropriate use shall result in limitation or cancellation of user privileges and possible disciplinary action, up to and including termination.

Internet mail and other Internet services are intended for CMC business purposes. It is recognized that some minimal incidental personal use may occur. However, regular non-CMC business usage of CMC-provided equipment, such as outside revenue generation or non-approved course/school/charitable work, needs to be authorized by the individual's immediate supervisor or by IT.

Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be intentionally sent either via email, viewed and downloaded, or passed by any other form of communication or displayed or stored on any CMC systems.

10. Hardware Use

Except for CMC-assigned laptops, CMC-owned computer equipment and peripherals may not be removed from the premises, relocated, or loaned to others without prior written authorization and/or approval from the Technical Services Desk and the immediate supervisor. Computers or peripherals not owned by CMC may be used on the College premises as a stand-alone device not connected to any CMC computer, network, or telecommunication system. With permission, some employees may be allowed to remotely access the CMC network by using a secure CMC-assigned virtual private network (VPN). However, Technical Support Desk personnel are not allowed to service any computer not owned by CMC. All computer equipment assigned to employees must be returned intact upon termination of employment.

11. Remote Access Phone Numbers and Internet Access Accounts

Remote system access, including phone numbers, VPN connections, Citrix connections, account IDs, and passwords are to be kept in strictest confidence. Users are not to give the connection ID, number,

address, or passwords to anyone else. Individuals, not employees, who need remote access, may request it from the Technical Support Desk. The use of modems is allowed only for system support by computer support personnel or for specific building/system alarms. No modem access is allowed for general users. All requests for remote access must be authorized in writing.

12. Security Violations

All CMC employees have a duty to immediately report all information regarding security violations or misuse of hardware or software to their supervisor and/or the Technical Services Desk.

The College President shall develop procedures as needed to implement this policy.