COLORADO COMMUNITY COLLEGE SYSTEM

SYSTEM PRESIDENT'S PROCEDURE

GENERAL COMPUTER AND INFORMATION SYSTEMS PROCEDURES

SP 3-125c

REFERENCE: BP 3-125; Electronic Communication Policy

EFFECTIVE: May 1, 2006

APPROVED: May 1, 2006
REVISED: August 4, 2008

S/ Dr. Nancy McCallin, System President

Purpose:

In support of its mission of teaching and community service, the Colorado Community College System (CCCS) provides access to computing and information resources for students, faculty, and staff within institutional priorities and financial capabilities. The Computer Use Procedure contains the governing philosophy for regulating faculty, student, and staff use of the System's computing resources. It spells out the general principles regarding appropriate use of equipment, software, networks and data. In addition to this policy all members of the CCCS community are also bound by local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media

The rules and conditions in the following document apply to all users of all systems in all locations of the Colorado Community College System. Willful violations of the following policies may result in disciplinary action following normal Human Resources procedures and guidelines in consultation with the appropriate supervisor, which may result in actions up to and including termination and necessary legal action.

Policy:

In accordance with the Colorado Open Records Act (CRS § 24-72-201 et seq.), it should be recognized that all public records are open for inspection by any person at reasonable times. The basic definition of "public records" in CORA is "all writings made, maintained, or kept by the state . . . ." This includes information and e-mail on state employees' computers. The only public records that fall outside this policy are records identified in specific exceptions set forth in CORA, in other Colorado statutes, and in federal law (including FERPA).

The CCCS has the right to monitor any and all aspects of its computer and telecommunications systems including employee e-mail, voice mail, and file structures on any CCCS system. CCCS's right to monitor its computer system and telecommunications equipment includes, but is not limited to, monitoring sites users visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users, and reviewing e-mail sent and received by users. The computer and telecommunication systems are provided to the employees to assist them in meeting the requirements for the performance of their positions in CCCS. Employees should not have an expectation of privacy in anything that they create, send, or receive on CCCS systems. Since systems are provided for CCCS business, all transactions and all data on the systems are considered to be business-related and therefore owned by the CCCS. All systems owned by CCCS are to be used for CCCS business purposes only. CCCS's control of all information on CCCS computers does not implicate intellectual property rights. Intellectual property rights are governed by Federal statutes and by the State Board for Community Colleges and Occupational Education's Policy 3-90.

Systems users should adhere to the following rules which apply to all computer and telecommunications resources including mainframe hosts, mid range hosts, micro computer hosts, file servers, desktops, notebooks, laptops, handheld devices, network infrastructure, PBXs, voice mail systems, Internet connectivity, bulletin board systems, e-mail systems and other resources.

This policy will be updated from time to time at CCCS's discretion. For example, changes to this policy will be made periodically by CCCS:

(a) When there is a change in applicable state or federal law;

(b) When new technology becomes available that increases CCCS's exposure to risks and consequently requires new control procedures.

Confidential Information

All employees and associates in the CCCS have an obligation (and are required by law) to keep confidential all information obtained from others, including student information (see FERPA Guidelines). Any questions regarding what information is public and available for sharing should be referred to your supervisor and/or the CCCS Legal Department. The confidentiality obligation also pertains to any party accessing any communication system.

User IDs and Passwords

All employees accessing any CCCS computer or communication system must have a unique User ID and Password. This includes user accounts for the Local Area Network,

Servers, and task-specific software applications such as SIS and FRS. To maintain system security, users are not to login as another user. Generic logins will not be issued unless an application, such as WebCT, requires it with no work-around. Each college should have a provision that open access computers for libraries are off the production network and are monitored for use.

The network and various application systems require all users to change their passwords every sixty days. Passwords must be at least 8 characters. Every password must contain at least 3 of the following 4 conditions: Upper-case characters, lowercase characters, numeric character, or special character (such as a numeric or punctuation character). Easily guessed passwords, such as the name of the user's spouse or child, their job title, their address, etc., should not be used.

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 that their password has been disclosed, they are required to change it immediately. User accounts are not transferable to temporary employees; if someone will be filling in for a user during an absence, a temporary account must be used for the interim employee. Security will be set up to make the user's data accessible by the person filling in.

Unattended Computers

To protect themselves and the confidentiality of data, users are required to logout, shut down their workstations, or activate a Windows screen saver with password protection when leaving their computers unattended, even if leaving for only a few minutes.

Logging Off / Shutting Down

Users are to completely log off and turn off their computers by selecting "Shutdown Computer" when leaving for the day. Users should always stay until their system shuts down according to the normal shutdown process. If the computer fails to shut down properly, the college's local computer support desk should be notified. Never turn off the power before the shutdown process is completed to avoid possible file corruption

Software

All users must comply with all software licenses, copyrights, and all other state and federal laws governing software licensing and intellectual property.
The installation, removal or copying of any software including customized programs, in-house developed applications, off the shelf software, gaming programs, public domain software (also known as shareware or freeware), or screen savers is prohibited by any user other than IT staff. Personal backgrounds or wall paper may be used subject to supervisor approval.

Exceptions are as follows:

- In areas where computer instruction is taught provisions will be made for the installation of software as part of normal classroom activities.
- Compiling any application as part of a classroom activity does not constitute the installation of software.
- Systems that are the sole property of agencies or institutions affiliated with CCCS shall be allowed to be administered by their own employees. These agencies are required to adhere to fundamental principles of good network neighbors in regard to virus checking, spam, etc. Typically these host servers will be secured in DMZ zones outside the production network.
- All institutions should ensure areas are set up so faculty and staff may review and demo software that may meet their needs.
- Exceptions can be made on a case by case basis to allow individuals power user permissions for operation of their computer system.

Internet and E-mail

Users may be granted access to the Internet for informational and business purposes.

The use of any CCCS resources for electronic mail is made available for College business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the College. Any such incidental and occasional use of College electronic mail resources for personal purposes is subject to the provisions of this policy.

All non-business usage, such as outside course/school or charitable work, would need to be authorized by the individual's supervisor.

Users are not allowed to download software from the Internet (including browser Plug-ins). If you require software to be downloaded that is on the Internet, please submit a request to the college's computer support desk for assistance.

Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent via e-mail, viewed and downloaded, or passed by any other form of communication or be displayed or stored. Exceptions may be made for various instructional purposes.
Creation and forwarding of non-business e-mail including advertisements, chain mail, solicitations, promotions, political material, etc., are not allowed.

Virus Protection

Various procedures are in place to protect the CCCS information systems from virus infection. Since floppy disks and USB drives can introduce a variety of malicious software into the campus network, users should exercise caution in their use of these devices. Any time a floppy disk or USB drive is used to transfer files it should be virus scanned prior to file copy.

All system hard disks will be scanned for viruses on a regular basis according to established standard procedures. Background scanning should always be enabled on client systems to check for viruses. If a virus is found, a message will be displayed and the file with the virus will be identified. If this happens, the user must call the computer support desk immediately and must not use the system until an authorized IT Technician has diagnosed and eliminated the virus.

Disabling or elimination of virus programs by users is considered a violation of procedure.

Hardware

CCCS-owned computer equipment and peripherals may not be removed from the premises, relocated, or loaned to others without prior written authorization from computer support desk or appropriately authorized individual. Some employees who travel frequently may be assigned a laptop or portable device by the employee's manager. Computers or peripherals not owned by CCCS may be used on the college premises only as a stand-alone device not connected to any CCCS computer, network or telecommunication system. Exceptions to this may be the connection of personal computers to projection systems or other devices that are not part of the production network. This must be supervised by a college employee. CCCS is not liable for any damages to personal systems used in this manner. Only Authorized IT Staff are allowed to install applications or configure these devices. Some employees may be allowed to connect either their own computers or college owned computers to CCCS network from home or when traveling on college business, using a secure CCCS-assigned VPN or Citrix software. However, computer support desk personnel are not allowed to service any computer not owned by CCCS

Personal Usage of Software/Hardware
CCCS-owned computer equipment and software applications may not be used for personal business at any time or for any reason, outside of incidental use. Any software not owned by CCCS may not be installed on CCCS-owned computer equipment. All computer equipment assigned to employees must be returned intact upon termination of employment.

Remote Access Phone Numbers and Internet Access Accounts

Remote system access including phone numbers, virtual private network connections, Citrix connections, phone numbers, account ID's, and passwords are to be kept in strictest confidence. Users are not to give the connection ID, number, addressing or the passwords to anyone else. Associates who need remote access may request it from the computer support desk. The use of modems will be allowed only for system support by computer support personnel or for specific building / system alarms. No modem access will be allowed for general users. All requests for remote access must be authorized in writing by the appropriate supervisor.

Backups

The computer support desk is responsible for performing nightly backups on network hosts and servers only. Local PC hard drives will not be backed up in any way. For this reason, the use of local PC hard drives for file storage is greatly discouraged. All users are required to log out of the system completely at the end of every work day. If a user has not properly logged out of the network at the time of backup, active files cannot be backed up. Confidential information, such as Family Educational Rights and Privacy Act (FERPA) information or Financial Aid information, should only be stored on secure servers, not on any individual's PC or on any portable electronic device.

Local PC hard drives will be erased when employment ends or the PC (Desktop PC, Laptop Computer, PDA, etc.) is taken out of service. Any data on the local PC hard drive is subject to loss and will not be recovered. Any work related documentation would be forwarded to the appropriate individual(s) designated by the supervisor.

Physical Security

Physical security is the first layer of control to restrict access to the information systems. All employees have a responsibility for security within the CCCS colleges' offices, computers and telecommunications facilities.

Inventory

All computers, peripheral devices (this includes PDAs, printers, computers, etc.) and telecommunication systems will be inventoried at a minimum once a year in accordance with Fiscal Policies for Fixed Asset Tracking. If systems cannot be accounted for by the department, the department management and the responsible employee or employees will be held accountable. Computer systems or equipment should not be moved or exchanged between employees without the notification and support of computer support desk.

Security Violations

All CCCS employees have a duty to report all information regarding security violations or misuse of hardware or software to either their supervisor and/or computer support desk immediately. Employees can also report security violations to the Employee Hotline.

Examples of Prohibited Activities

Prohibited activities on CCCS computers and telecommunications systems include but are not limited to:

Sending, receiving, displaying, printing, otherwise disseminating, or storing material that is fraudulent, harassing, illegal, abusive, indecent, embarrassing, profane, sexually

explicit, obscene, intimidating, or defamatory; Exceptions may be made for legitimate instructional purposes.

Transmitting to others, in any location, images, sounds or messages that might reasonably be considered harassing;

Screen displays of images, sounds or messages that could create an atmosphere of discomfort or harassment for others, especially those considered obscene or sexually explicit;

Attempting to forge electronic mail messages or using someone else's electronic mail;

Accessing personal interest sites, viewing chat rooms (except chat rooms integrated within the course management system), or using recreational games for other than occasional use.

Using CCCS computers for commercial gain or private profit;

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, music, videotapes, books, or other copyrighted sources, and copyrighted software;

Exporting software or technical information in violation of U.S. export laws;

Posting or e-mailing scams such as "make money fast" schemes or pyramid/chain letters;

Threatening bodily harm or property damage to individuals or groups;

Making fraudulent offers of products, items, or services originating from a user's account;

Attempting to access the accounts of others, or attempting to penetrate security measures of other entities' systems ("hacking"), whether or not the intrusion results in corruption or loss of data;

Accessing another person's computer, computer account, files, or data without permission;

Using any means to decode or otherwise obtain restricted passwords or access control information;

Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain access to any system;

Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., “spamming”, “phishing”, “flooding”, or “bombing”);

Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to data;

Engaging in any other activity that does not comply with the general principles presented above.

Frequently Asked Questions and Answers

1. Why does the IT computer use policy apply to my telephone? My fax machine?

Both your telephone and your fax machine are electronic communication resources and fall under the definition of IT resources. A single policy was written for all IT resources in order to address related policy issues and to make it easier for users to be informed of policy requirements.

2. Does the IT policy apply to the computer I purchased for my home, using my own money?

No, since you paid for your computer from your own funds, the policy doesn't apply to it. However, if you use your computer to connect to a CCCS IT resource, such as the data communications network, the policy applies to any action you take via your computer on that resource.

3. If I use the CCCS network to connect to an IT resource that belongs to someone else, whose policy applies to my actions?

Suppose you use the CCCS network to connect to a database belonging to another institution. Both the CCCS IT policy and any policies of the other institution apply to your actions. Depending on what you do while connected to that database, Federal or state laws could also be applicable. It's very hard to find, read, and understand everything that may apply. If you adhere to high standards of ethical and responsible behavior you're unlikely to commit a serious infraction of any of the policies, rules, or laws.

4. Does the hardware and software purchased by my department from grant funds belong to CCCS?

Yes, it does. The grant funds are almost certainly money provided under a contract between the CCCS college and the grant source. As such, they are monies of the CCCS college and anything purchased or leased or created through the use of that money belongs to the CCCS. So this policy applies, and CCCS has the right to access that hardware and software as may be necessary.

5. Who is and who is not a user of CCCS IT resources?

Anyone who uses the CCCS data communication network to access data at another institution is a user.

Anyone who stores data files on the CCCS network is a user.

Anyone who uses a computer in a CCCS college lab is a user.

An employee who uses a home computer they purchased themselves to access the web through a commercial Internet Service Provider is not a user of IT resources at that time.

6. Does CCCS have the right to look at my accounts, files, and electronic communications?

Yes, CCCS officials have a right to look at any user's electronic accounts, files, or communications within the limits established by law. Employees need to understand that there is no absolute right to personal privacy when the employee is using the employer's equipment, including IT resources. CCCS does not routinely monitor the content of files or communications, but may view contents whenever it has a business or legal need to do so.

You should also be aware that the files you maintain on CCCS IT resources may be considered public records and the CCCS may be required to make them available for inspection under the Colorado Open Records Act. In addition, the Act defines "public records" to include electronic mail messages which means that your email messages also may be subject to public inspection.

7. What about my right to privacy? Does CCCS protect the confidentiality of data about me?

The current state of IT is such that there can be no absolute assurance of privacy or confidentiality of electronic data and systems. CCCS takes reasonable and prudent precautions to protect privacy, but users should understand there is always some risk that data can be accessed by unauthorized people.

8. Does CCCS have the right to delete my data or block my communications?

CCCS IT administrators are charged with maintaining and operating the resources for the benefit of all members of the CCCS colleges. If someone's data consumes so much storage that others are denied storage or if someone's web page attracts so much network traffic that others are denied network access, the administrator of those resources has the right to remove the material. Whenever possible, users are given an opportunity to backup data to other media before it is removed.

9. Can I trust the CCCS to take care of the files I store on its IT resources?

CCCS IT administrators take reasonable and prudent steps to protect the integrity of data and systems stored on the resources they administer, but there is always some risk that files may be lost or damaged. Users are urged to make backup copies of their personal files that would be difficult or costly to replace.

10. What are some examples of how to create a password using the Password Standards?

The use of words and phrases is acceptable if they are not easily guessable and contain a combination of upper case, lower case, numerals, and special characters. In some cases you can substitute numerals for letters. For example: Th1s1saTest, or th1Sisat3st, or tHisisAt3st, or This1s.atest

11. Who can work on equipment?

CCCS faculty, staff and student may use computers as per SP 3-125c, However, only certified IT Staff can service state owned computers, printers, projectors, PDAs, etc. This includes installation of software applications (i.e., Microsoft Word, Excel, Adobe PhotoShop, etc.) CCCS IT Staff will not support computers, PDAs, etc. that do not belong to CCCS.

12. What is the difference between Programs or Executables vs. Content?

Programs or Executables generally require installation on the computer and generally require licensing. Content is the files that can be opened by an application. Examples: Microsoft PowerPoint is the “application” required to create, open and modify PowerPoint presentations. PowerPoint files that are created by the application are the “content.” Often textbook series include PowerPoint files. If PowerPoint is not installed on the machine, the computer cannot open the files. Test banks (“applications”) are what generate test questions. If you can save those questions, that file is the “content.”

13. Who installs updates, browsers and plug-ins?

Only IT Staff are allowed to install updates, browsers and plug-ins. Some updates, plug-ins, etc. may be installed through a variety of methods that will not require user intervention.