

PROCEDURE NAME: District Network and Computer Use

Introduction: *Chaffey College has a strong commitment to providing a quality education for its students, including access to and experience with current technology. The District's goals for technology in education include providing access to all students, faculty and staff, fully integrating technology into the daily curriculum and preparing students and educators to meet the challenge of a highly technological and information-rich classroom and workplace.*

Authorization: This procedure is authorized by Board Policy 3.10 Computer Use. Employees and students who use district computers and networks and the information they contain, and related sources, shall not abuse those resources and will respect the rights of others. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users. This is an Information Technology Services department procedure that can be modified through the Technology Committee.

Definitions: Definitions and concepts used within this procedure are applied using a "reasonable person standard" within the context of professional practice.

Purpose: To inform all District students, faculty, staff and others of the proper use of District information resources whether these resources are individually controlled, shared, stand-alone or networked. This procedure encompasses the use of personal computers, desktops, laptops, workstations, associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

1. This procedure applies to:
 - all District students, faculty, staff and others granted the use of District information resources and
 - all computer and computer communications facilities owned, leased, operated, or contracted by the District.
2. The District computer and network systems are owned by Chaffey Community College District. All individuals must have proper authorization in order to use these resources. The computer and network resources are for District instructional, educational and work-related purposes only. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct inappropriate activities within those domains.
3. Conditions of Use
 - 3.1 When using the District network and computers, all users are expected to follow the rules contained in this procedure and to use the network and computers in an ethical and lawful manner. Individual departments within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.
4. Legal Process
 - 4.1 A user of District information resources who is found to have violated any of these policies or procedures will be subject to established disciplinary action.
5. Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other online information.

- 5.1 Copying – Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied to, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law. Computers used by students are locked down; therefore downloading and installing software applications onto district computers is not acceptable except when supervised by faculty as part of the curriculum. Downloading software applications for staff is not acceptable unless prior approval has been obtained from the supervisor or system administrator. Faculty may download files and/or software applications on their assigned workstations as deemed necessary. Automatic software updates for currently owned software is acceptable. All software applications downloaded must conform to copyright and license restrictions.
- 5.2 Number of Simultaneous Users – The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department and/or District does not exceed the number of original copies purchased by that department and/or District, unless otherwise stipulated in the purchase contract or licensing agreement.
- 5.3 Copyrights – In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from the computer or network resources must be used in conformity with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

6. Integrity of Information Resources

Computer users are responsible for maintaining the integrity of computer-based information resources.

- 6.1 Modification or Removal of Equipment – Prior authorization from the supervisor or system administrator is required to modify or remove computer equipment, software, or peripherals. It is recognized that portable equipment or equipment for which one has personal responsibility (e.g. a laptop) may be moved. Definitions and concepts are applied using a “reasonable person standard within the context of professional practice.”
- 6.2 Unauthorized Use – Computer users will use the district system in a manner consistent with their work assignment. Users must not interfere with others’ access and use of District computers. This includes, but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

- 6.3 Unauthorized Programs – Computer users are expected to access authorized programs only. Users must ensure that they do not use programs or utilities that interfere with other computer users, or that modify normally protected or restricted portions of the system or user accounts. Computer users must not intentionally use programs which disrupt other computer users, or which access private or restricted portions of the system, or which damage the software or hardware components of the system.
- 6.4 Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.
- 6.4.1 Abuse of Computing Privileges – Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs, or the computers at other sites connected to those networks, will be treated as an abuse of District computing privileges.
- 6.4.2 Reporting Problems – Any defects discovered in system accounting or system security should be reported promptly to the appropriate system administrator and/or supervisor so that steps can be taken to investigate and solve the problem.
- 6.4.3 Password Protection – A computer user who has been authorized to use a password-protected account will be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the supervisor or system administrator. Generic user accounts and passwords by definition are shared with appropriate and authorized users.

7. Usage

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

- 7.1 Unlawful Messages – Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.
- 7.2 Obscene Material – Creating, transmitting, viewing, uploading, or downloading of obscene materials is strictly prohibited. Use of computers to research material associated with instructional assignments is permitted.
- 7.3 Information Belonging to Others – Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.
- 7.4 Rights of Individuals – Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.

- 7.5 User Identification – Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.
- 7.6 Political Use – The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters. District information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws.
- 7.7 Personal Use – Occasional personal use of the computer and associated resources is authorized as long as it does not distract from work-related activities. Participation in online or electronic CHAT is only allowed for Chaffey business-related purposes.
- 7.8 Personal Computers
Only district approved and certified equipment shall be connected to the District network. Personal computers or other network devices are not to be connected to the District network. District loaner laptops are available for checkout from departments when the facility/location used does not have access to a permanent computer.

8. Nondiscrimination

- 8.1 All users have the right to be free from conduct which harasses or discriminates against any person on the basis of race, color, creed, national origin, ancestry, gender, marital status, disability, religious or political affiliation, age (over 40), sexual orientation, medical condition or military status as a Vietnam era veteran as required by all federal and state laws that is connected with the use of the District's network and computer resources.
- 8.2 No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

9. Disclosure

- 9.1 Privacy – The District reserves the right to monitor all use of the District network and computer system if abuse is suspected, to assure compliance with these policies and procedures, to maintain system integrity, to ensure system security and to promote best business practices. The District will exercise this right only for legitimate District purposes. This provision does not replace or supersede established disciplinary processes as outlined in all known negotiated contracts. Those with administrator access will not view employees' mail without authorization from the Superintendent or his/her designee.
- 9.2 Possibility of Disclosure – Users must be aware of the possibility of unintended disclosure of communication.

- 9.3 Retrieval – It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.
- 9.4 Public Records – The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of “public record” and nonexempt communications made on the District network and computer system must be disclosed if requested by a member of the public.
- 9.5 Chaffey College reserves the right to employ software for use in filtering unwanted, unsolicited, harmful, or otherwise inappropriate material following established District process.

10. Dissemination and User Acknowledgment

- 10.1 All users shall be provided copies of these procedures and be directed to familiarize themselves with them.
- 10.2 Prior to receiving an account on the District network and computer system, users must sign a statement acknowledging that they have read and will comply with the District’s Computer Use policy and associated procedures. In addition, they must acknowledge receipt of the Accountability Statement and will comply with the following requirements:
 - a. Passwords and/or codes will not be shared with other employees or students.
 - b. Confidential data will be disposed of in an approved manner.
 - c. Creation or transmission of any false statement which tends to cause injury to one’s reputation is strictly prohibited.
 - d. Creating, transmitting, uploading or downloading obscene materials is strictly prohibited.
 - e. Use of the District computers/networks is for college-related activities only.
- 10.3 An initial screen addressing a synopsis of these procedures shall be installed on computers with access to the administrative information system. This screen shall appear prior to accessing the administrative information system. Users must positively acknowledge the statement that they have read and understand this procedure and that they will comply with it. A user acknowledgment shall be in the form as follows:

“The information you are requesting to access is protected by State and Federal law and is regarded as confidential by the District.

You must agree to:

- Access only the information needed to complete your assigned authorized task(s),
- Collect and retain only such information as is needed to effectively conduct District business,

- Handle such information in a secure, confidential and appropriate manner in compliance with relevant laws, regulations, policies and procedures, and
- Protect the privacy of employee and/or student records, and prevent inappropriate or unnecessary disclosure of such records.

You must acknowledge the following:

I understand that by proceeding into the Chaffey College District software system, I agree to comply with the above and understand that if I fail to abide by these conditions, my access to all District information systems may be terminated and that I may be subject to formal disciplinary action.”

Type 'Y' to accept or 'N' to logoff.

11.0 Chaffey E-Mail Usages

11.1 Ownership

Chaffey College owns the e-mail system and is ultimately responsible for its use and content.

11.2 Personal Use

- Occasional personal e-mail is authorized as long as it does not distract from work-related activities.
- E-mail is a business tool entirely owned by the district, which reserves the right to monitor mail should policy abuse be suspected.
- Mail containing lewd or inappropriate content is unacceptable.
- Chain letters are prohibited.

11.3 Privacy

- Those with administrator access to mail will not view employees' mail without authorization from the Superintendent or his/her designee.
- Those with administrator access may also view employees' mail at the request of the user/owner of the email.
- In accordance with 9.1, the district retains the right to monitor mail.
- Users must take steps to ensure that their password is unique and that it stays private.
- Users are forbidden to give their password to others without permission of the supervisor or system administrator.

11.4 E-Mail Features and User Responsibilities

- District e-mail offers a variety of features including return receipt, blind carbon copy and urgent delivery. Use of all features is authorized but employees should be judicious in the use of these features since they increase mail traffic and may take priority in mail queues.
- Use of graphics and sounds should be avoided as even small items can greatly increase the message size.
- Transmissions of graphics, audio or other sizable files should be kept to a minimum.
- Attachments from graphic-intensive programs such as PowerPoint should be zipped before sending.

- Prudence must be exercised in using global distribution lists. Mass mailings increase traffic in the system and are often not appreciated by the recipient.
- Large attachments should be used sparingly on global distribution lists. The size limit for an email sent to a distribution list is 300 Kb.
- Topics must be business related.
- Content must be timely and contain current information.