

AP 3720 Computer and Electronic Communication Systems

Reference:

Education Code Section 70902

- 1.0 This procedure applies to all District students, faculty and staff and to others granted use of District computer and electronic communication systems. This procedure refers to all District computer and electronic communication systems whether individually controlled or shared, stand-alone or networked.
- 2.0 **Definitions**
 - 2.1 For purposes of this policy, electronic communications, electronic communication services or electronic communication systems include, but are not limited to, electronic mail, electronic mail address or account, District computer systems, Internet services, voice mail, audio and video conferencing, and facsimile messages.
 - 2.2 The District's computer systems include, but are not limited to, any and all District-owned, leased, or rented computer hardware, software, databases, telecommunications equipment, telephone and related equipment, and any system used in connection with District programs.
 - 2.3 E-mail means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval. E-mail includes electronic messages that are transmitted through a local, regional, or global computer network.
 - 2.4 Voice mail means an audio message transmitted telephonically between two or more telephones, whether or not the message is converted to hard copy format after receipt and whether or not the message is heard upon transmission or stored for later retrieval. Voice mail includes telephonic messages that are transmitted through a local, regional, or global telephone network.
- 3.0 **District Property**
 - 3.1 District Electronic Communication Systems and services are District property. Any electronic mail address or account associated with the District, or any sub-unit of the District, assigned by the District to individuals, sub-units, or functions of the District, is the property of the District.
 - 3.1 Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

AP 3720 Computer and Electronic Communication Systems

4.0 Service Restrictions

- 4.1 Users of the District's computer and Electronic Communication Systems and services are expected to do so responsibly and in compliance with state and federal laws, policies and procedures of the District, and with normal standards of professional and personal courtesy and conduct. Access to District electronic communications services is a privilege that may be wholly or partially restricted by the District without prior notice and without the consent of the user. Reasons for restricting access to the electronic communications services include, but are not limited to, the following: when required by and consistent with law; when there is significant reason to believe that violations of policy or law have occurred; when failure to act may result in significant bodily harm; when significant property loss or damage would result; when loss of significant evidence of one or more violations of law or of District policies would result; when significant liability to the District or to members of the District community would result; or District business operational needs warrant.
- 4.2 Electronic communications access privileges may not be transferred or converted to other Individuals. An account assigned to an individual shall not be used by any other person without explicit permission from the systems administrator.
- 4.3 Users should be aware that the electronic communication systems are not private. Unsecured electronic communication systems should not be used to transmit confidential information about students, employees, or District affairs. For purposes of this provision, confidential information includes, but is not limited to, the address, telephone numbers, and personal or private facts of students or employees.

5.0 District Access and Disclosure

- 5.1 Users should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the District's computer system or stored in the users' directory.
- 5.2 Although the District does not routinely inspect, monitor, or disclose electronic communications, the District reserves the right to inspect, monitor, or disclose electronic communications without prior notice and without consent. Reasons for inspecting, monitoring or disclosing electronic communications include, but are not limited to, the following: when required by and consistent with law; when there is significant reason to believe that violations of policy or law have occurred; when failure to act may result in significant bodily harm, when significant property loss or damage would result, when loss of significant evidence of one or more violations of law or of District policies would result, when significant liability to the District or to members of the District community would result; or significant liability to business

AP 3720 Computer and Electronic Communication Systems

purposes, such as inspection of the contents of electronic messages in the course of an investigation triggered by indications of misconduct. Such inspections must be authorized by the Chancellor, Vice Chancellor, College President, or Provost of Continuing Education. The inspection must be limited to materials related to the investigation and the confidentiality of the inspection must be maintained to the highest degree possible. In the event a search of computer files is authorized, a reasonable effort must be made to secure technical assistance from a site other than the site of the employee whose files are being searched.

6.0 Use Disclaimer

- 6.1 Both the nature of electronic communications and the public character of the District's business do not provide privacy for electronic communications, and confidentiality of electronic communications should not be expected. Users, therefore, should exercise extreme caution in using electronic communications to communicate confidential or sensitive matters. In addition to the District's right to inspect, monitor, or disclose electronic communications without prior notice and without consent, routine maintenance or system administration of computers and other electronic communications equipment may result in observation of the contents of files and communications.
- 6.2 Electronic communications that utilize District equipment, whether or not created or stored on District equipment, may constitute a District record subject to disclosure under the California Public Records Act or other laws, or as a result of litigation.
- 6.3 The District cannot protect users from receiving electronic communications they may find offensive, nor can the District guarantee the authenticity of electronic communications received, or that electronic communications received were in fact sent by the purported sender. Users are solely responsible for materials they access and disseminate on the District's Electronic Communication Systems.
- 6.4 It is possible for information entered on or transmitted via computer and communication systems to be retrieved, even if a user has deleted such information.

7.0 Acceptable Use

This section defines acceptable use of the District's electronic communication services and computer systems. It does not articulate all permissible and prohibited uses, but is intended to provide a framework to guide users that is based on honoring the rights of other users, respecting the integrity of the systems, and observing relevant laws, regulations, contractual obligations, and Board Policies.

AP 3720 Computer and Electronic Communication Systems

7.1 Purpose

Electronic communication services are provided by the District in support of the academic, research, and public service mission of the District, and the administrative functions that support this mission.

7.2 Users

Users of District electronic communication services are limited to District students, faculty, staff and other authorized persons. Use is limited to purposes conforming to the requirements of this section.

8.0 Unacceptable Use

The use of District computer systems and electronic communication systems and services for any of the following is prohibited:

- 8.1 Any purpose which violates state or federal law including, but not limited to, violation any District or other computing and/or network system;
- 8.2 Violation of software licensing agreements, using software without obtaining legal authorization, or unauthorized duplication, transmission, or use of unlicensed copies;
- 8.3 Private commercial purposes not under the auspices of the District;
- 8.4 Personal financial gain;
- 8.5 Any purpose that could reasonably be expected to interfere with or disrupt use of the Electronic Communication Systems or cause, directly or indirectly, excessive strain on any computing facilities, or unsolicited interference with others' use of the system, including, but not limited to, the following:
 - 8.5.1 Knowingly sending or forwarding "junk" e-mail or mass electronic mailings, such as chain letters;
 - 8.5.2 Exploiting list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail ("spam");
 - 8.5.3 Knowingly resending the same e-mail repeatedly to interfere with a recipient's use of e-mail ("letter-bomb");

AP 3720 Computer and Electronic Communication Systems

- 8.5.4 Knowingly loading virus programs onto or from any computer system (viruses);
- 8.5.5 Attempting unauthorized access or alteration to data, files, passwords or breach of security measures on any electronic communication systems, or attempting to intercept, eavesdrop, record, read, receive or alter other person's e-mail without proper authorization (hacking);
- 8.5.6 Unauthorized tampering with computing resources, including connecting or disconnecting computer equipment or otherwise altering the set-up of any computer or network of computers;
- 8.6 Reposting personal communications without the author's prior consent;
- 8.7 Advertising, campaigning, soliciting or proselytizing for any religious or political cause, outside organization, or individual;
- 8.8 Personal use inconsistent with section 10.0 of this procedure;
- 8.9 Sending defamatory, intimidating, threatening, harassing, discriminatory, abusive or patently offensive material to or about others, sending messages that disclose personal information without authorization, or sending material that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion or political beliefs;
- 8.10 Sending or accessing pornography or patently obscene material other than for authorized research or instructional purposes;
- 8.11 Downloading of unlicensed or copyrighted movies or music for other than legally authorized uses, or uses authorized by the District.
- 8.12 Any use that violates District policies or guidelines including, but not limited to, policies or guidelines regarding intellectual property, nondiscrimination, or sexual or other forms of harassment.
- 8.13 For purposes of this section, use of District electronic communication systems means to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, access or print. A User is an individual who makes use of District electronic communication services.

9.0 Representation

Users of the District's electronic communication services shall not give the impression that

AP 3720 Computer and Electronic Communication Systems

they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the District unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included.

10.0 False Identity

Users of the District's electronic communication services shall not employ a false identity or otherwise transmit or attempt to transmit any message which is misleading as to origination.

11.0 Personal Use

11.1 The District's electronic communication services are provided to support the educational mission of the colleges and the School of Continuing Education. The electronic communication services are to be used primarily for school-related purposes. Incidental personal use is permitted provided that the incidental personal use conforms to this policy and such use does not:

11.1.1 Interfere with the user's employment or other employees;

11.1.2 Directly or indirectly interfere with the District operation of computing facilities or electronic communication services;

11.1.3 Burden the District with noticeable incremental cost.

11.2 Electronic communication records arising from such personal use may be presumed to constitute District records subject to the potential for disclosure under the California Public Records Act. Users should assess the implications of this presumption in any decision to use District electronic communication services for incidental personal purposes.

12.0 The District's computer systems provide access to local, national and international sources of information in an atmosphere that encourages access to knowledge and sharing. The District supports an intellectual environment in which students, staff and faculty may create and collaborate with colleagues without fear that the products of their efforts will be violated by misrepresentation, tampering, destruction and/or theft. However, users are solely responsible for the material that they access and disseminate on the District's computer systems.

13.0 Policy Violations

Violations of District policies and procedures governing the use of District computer systems and electronic communication services may result in the temporary or permanent restriction of access to District computer systems and electronic communication services and

North Orange County Community College District
ADMINISTRATIVE PROCEDURES
Chapter 3
General Institution

AP 3720 Computer and Electronic Communication Systems

appropriate disciplinary action, up to and including student dismissal or employee termination in accordance with existing board policies and State Education Code. Violation of state or federal law may result in reporting the violation to the appropriate law enforcement agencies.

- 14.0 Users shall sign and date the acknowledgment and waiver included in this procedure, and will comply with it.

Date of Adoption: March 23, 2004

North Orange County Community College District
ADMINISTRATIVE PROCEDURES
Chapter 3
General Institution

AP 3720 Computer and Electronic Communication Systems

Computer and Electronic Communication Systems Agreement

I have received and read a copy of the District Computer and Electronic Communication Systems Procedures and this agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Electronic Communication Systems Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.

Signature