
Administrative Procedure
Chapter 3 – General Institution

AP 3720 COMPUTER AND NETWORK USE

References:

17 U.S. Code Sections 101 et seq.;

Penal Code Section 502, Cal. Const., Art. 1 Section 1;

Government Code Section 3543.1(b);

Government Code Sections 6250 et seq. (California Public Records Act);

Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

NOTE: *The following language in red ink is legally advised. The Policy & Procedure Service updated the language in red ink (below) in September 2005, August 2006, February 2007, April 2014, November 2014, October 2015, and October 2017. Local practice may be inserted. The following is an illustrative example:*

The District Computer and Network systems are the sole property of the Napa Valley Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are intended for District instructional and work related purposes only.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, electronic mail, Internet and intranet service, District operated social media sites, voice mail, audio and video communications, facsimile messages, personal computers, workstations, laptops, tablets, cell phones, mainframes, virtual hosts, virtual machines, minicomputers/servers, and associated peripherals, software and information resources including offsite storage, regardless of whether used for administration, research, teaching, or other purposes.

CONDITIONS OF USE

Individual units 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, or restrictions.

DISCIPLINE AND LEGAL PROCESS

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action. Also see BP/AP 7360 Discipline and Dismissals – Contract/Regular Faculty (Academic Employees), BP/AP 7365 Discipline and Dismissals – Classified Employees, and BP/AP 5500 Standards of Student Conduct.

COPYRIGHTS, LICENSES, AND OWNERSHIP

Computer users must respect copyrights and licenses to software and other on-line information.

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 into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

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 does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance 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. Also see BP/AP 3710 Securing of Copyright.

Ownership – BP/AP 3720 is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, and all hardware and software components within it, is the sole property of the District which sets the terms and conditions of its use consistent with the law. Except as provided in other Board Policy pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the District Network. Also see BP/AP 3715 Intellectual Property.

INTEGRITY OF INFORMATION RESOURCES

Computer users must respect the integrity of computer-based information resources.

NOTE: *Districts may reference the electronic information security standard created by the California Community Colleges Technology Center. The California Community Colleges Technology Center has helpful information on this subject, which can be accessed on their website.*

Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

Unauthorized Use - Computer users must not interfere with others access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; **utilization of distribution lists, either local or external, outside of their work-related purpose or guidelines**; printing excess copies of documents, files, data, or programs, 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.

Unauthorized Programs - Computer users must not intentionally develop or 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. Computer 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. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access - Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

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.

Reporting Problems - 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.

Password Protection - A computer user who has been authorized to use a password-protected account may 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 system administrator.

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.

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.

Commercial Usage - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public discussion groups have been designated for selling items by/ **insert names of groups, if any** and may be used appropriately, according to the stated purpose and guidelines of the group(s).

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.

Rights of Individuals - Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization. Also see BP/AP 5040 Student Records, Directory Information, and Privacy.

User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

POLITICAL, PERSONAL, AND COMMERCIAL 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.

Political Use - District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

Personal Use - District information resources should not be used for personal activities not related to District functions, except in a purely incidental manner. For District employees, the intended uses of the District Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional activities. Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities provided that such use is within reason and provided that such usage is ordinarily on an employee's own time, is occasional, and does not interfere with or burden the District's operation. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.

Public Use - The Napa Valley Community College District has computers available in designated areas to serve the educational, informational, and recreational needs of the community and have been identified for "public use". On selected computers access is provided to Internet and library resources such as reference databases of general and special periodical materials as well as archival information. Material on the Internet is not pre-screened, monitored, censored, endorsed or ratified by the District. The District waives any responsibility for content accessible from the Internet. Public use computers may have additional conditions for use, but the fundamental principles related to legal compliance, integrity of information resources, nondiscrimination, and general disclosure as outlined in this procedure are considered applicable to any such users who have been granted use of District computers and network resources. Violations may result in revocation of utilization privileges and/or immediate termination of the violator's relationship with the District and could lead to civil or criminal prosecution.

Commercial Use - District information resources should not be used for commercial purposes. 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 activities not authorized within those domains.

NONDISCRIMINATION

All users have the right to be free from any conduct connected with the use of the Napa Valley Community College District network and computer resources which discriminates against any person on the basis of national origin, religion, age, gender, gender identity, gender expression, race, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, pregnancy, or military and veteran status, or because he/she is perceived to have one or more of the foregoing characteristics, or because of his/her association with a person or group with one or more of these actual or perceived characteristics. 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. Also see BP/AP 3410 Nondiscrimination.

DISCLOSURE

No Expectation of Privacy - The District reserves the right to monitor all use of the District network and computer to assure compliance with this procedure and the related policy. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure - Users must be aware of the possibility of unintended disclosure of communications.

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.

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 or computers must be disclosed if requested by a member of the public. Also see BP/AP 3300 Public Records.

Litigation - Computer transmissions and electronically stored information may be discoverable in litigation.

Loss of data - The District assumes no responsibility for the loss of data on individual owned or district owned computer and computer communication systems due to computer viruses or other destructive software, or as a result of flaws in the application or operating system software.

Electronic Communication Limitations - 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 responsible for materials they access and disseminate on the District’s computer and electronic communication systems.

Authorized use by minors - All students under the age of eighteen, by accepting the benefits of authorized use of the District's technology resources, acknowledge that material inappropriate for minors is accessible on the Internet; that various wrongdoing, such as identity theft, invasion of privacy and fraud, may occur on the Internet, and that their use of the Internet may therefore expose them to a variety of risks of harm to person or property. By using the District’s technology resources, minors and their parents accept responsibility for any and all risks thereof and acknowledge that the District shall not be responsible for any harm or damage resulting from such use.

DISSEMINATION AND USER ACKNOWLEDGMENT

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

A “pop-up” screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The “pop-up” screen shall appear prior to accessing the e-mail network. Users shall sign and date the an acknowledgment and waiver included in this procedure stating that they will comply with it. This acknowledgment and waiver shall be in the form as follows:

Computer and Network Use Agreement (Sample Language)

I have received and read a copy of the District Computer and Network Use 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 or enrollment. I am aware that violations of this Computer and Network Usage 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 or Federal law.~~

[Also see AP 6365 Accessibility of Information Technology.](#)

NOTE: The **red ink** signifies language that is **legally advised** and recommended by the Policy & Procedure Service and its legal counsel (Liebert Cassidy Whitmore). This procedure reflects updates/revisions from the Policy & Procedure Service in September 2005, August 2006, February 2007, April 2014, November 2014, October 2015, and October 2017. The language in **blue ink** is included for consideration. The language in **yellow highlighting** is included to draw the reviewers' attention, and this language will be removed upon final document approval. The language in **green ink** is local edits made including any strikethrough text.

Approved:

(**This is a new procedure**)