



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

The District computer and network systems are the sole property of the District. They may not be used by any person without the proper authorization of the District. The computer and network systems are for District instructional and work-related purposes only.

For the purposes of this procedure, a computer is defined as any device that accesses District software and/or resources.

This procedure applies to all District students, employees, and others who are granted use of the District's 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 personal computers, workstations, mainframes, minicomputers, and associated peripherals, software, and information resources, regardless of whether used for administration, research, teaching, or other purposes.

Conditions of Use

Operational and departmental units within the District may define additional conditions of use for information resources under their control. Such statements must be consistent with this overall procedure but may provide additional detail, guidelines, or restrictions.

Legal Process

This procedure exists within the framework of the District's BP 3720 Computer and Network Use and state/federal laws. A user of District information resources who is found to have violated BP 3720 Computer and Network Use or this procedure 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.

Copyrights and Licenses

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

Integrity of Information Resources

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

Modification or Removal of Equipment

Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by the District without proper authorization.

Unauthorized Use

Computer users must not interfere with others' access to and use of the District's computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; 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.

District computer and network systems shall be used only for college-related purposes and shall not be used to engage in activities that are against federal, state, local laws, Board policies or Administrative Procedures. Unauthorized use includes, but is not limited to, engaging in harassing, intimidating, or bullying behavior, the viewing of obscene materials, behavior that violates sexual harassment laws, and discrimination based on any protected classes.

Unauthorized Programs

Computer users must not intentionally develop or use programs which disrupt other computer users, access private or restricted portions of the system, or 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 Information Technology Division 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.

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.

Prohibited 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/procedure, 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). Public discussion groups may be created and designated for selling items and may be used appropriately, according to the stated purpose 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 student's or employee's personal information to anyone without proper authorization.

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, computers, and devices should not be used for personal activities not related to District functions, except in a purely incidental manner.

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 District’s network and computer resources which discriminates against any person. (See BP 3400 Protected Classes.)

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.

No Expectation of Privacy

The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. 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.

Litigation

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

Dissemination and User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them. All employees shall submit a signed agreement to the terms of use outlined in this procedure.

A notice addressing these procedures shall be presented at the login screen of the District-wide authentication portal. The notice shall appear prior to accessing all portal applications. Accessing District computing resources implies acknowledgement, acceptance, and agreement to these procedures.

FEDERAL, STATE, AND DISTRICT STATUTES, REGULATIONS, AND POLICY REFERENCES

The following is a partial list of Federal, State, and District statutes, regulations, and policies that pertain to the District’s Computer Use Policy and Procedures. This list of references does not include all Federal, State, and District statutes, regulations, and policies that pertain to this procedure.

State of California Statutes

State of California Information Practices Act of 1977 (Civil Code Sections 1798 et seq.)
State of California Education Code Sections 67100 et seq.



State of California Education Code 92000
State of California Government Code Section 11015.5
State of California Penal Code Section 502
State of California Public Records Act (Government Code Sections 6250 et seq.)
The California Community Colleges Technology Center's Electronic Information Security Standard

Federal Statutes and Regulations

American with Disabilities Act of 1990
Communications Decency Act of 1996
Copyright Act of 1976 Digital Millennium Copyright Act of 1998
Electronic Communications Privacy Act of 1986 Electronic and Information Technology, Section 508
Family Educational Rights and Privacy Act of 1974
Federal Communications Commission Rules and Regulations Federal Copyright Act of 1976
Privacy Act of 1974
Telecommunications Act of 1934
Telecommunications Act of 1996
District Policies (Note: Correct listing of relevant District Policies will be referenced in this Appendix)
BP 4030 Academic Freedom
Disciplinary Procedures, Policies for Faculty and Educational Administrators, section 2500, Appendix F
AP 5520 Student Discipline Procedures
BP/AP 3410 Nondiscrimination
Faculty Grievances, Policies for Faculty and Educational Administrators, section 2500, Appendix F
BP/AP 3900 Speech: Time, Place, and Manner
BP/AP 3715 Intellectual Property
Freedom of Expression, Policies for Faculty and Educational Administrators section
BP/AP 5500 Student Conduct
AP 5530 Student Rights and Grievances
BP 1100 Santa Barbara Community College District

Date Approved: June 13, 2016
Legal Reference Update #25: November 2014
Date Revised: September 27, 2017