General Institution

AP 3720 INFORMATION TECHNOLOGY USE

References:

Government Code Section 3543.1(b);
Penal Code Section 502;
17 U.S. Code Sections 101 et seq.;
Cal. Const., Art. 1 Section 1;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, and 45;
Homeland Security Act;
CALEA (Communications Assistance for Law Enforcement Act);
FERPA (Family Educational Rights and Privacy Act);
ACCJC Guide to Evaluating Distance Education and Correspondence Education

All information technology resources, including computers, networks, and learning management systems, are the sole property of the District. They may not be used by any person without the proper authorization from the District.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. These procedures govern desktop, network, email, telephone, internet, data security, and software uses of College-managed information technology equipment and resources.

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, and/or restrictions.

Legal Process
This procedure exists within the framework of the District Board Policy and local, state, and federal laws. A user of District information technology resources who is found to have violated these procedures will be subject to disciplinary action; loss of information resources privileges; and/or civil or criminal legal action.

Copyrights and Licenses – Information technology users must respect copyrights and licenses to software and other online information.

Copying – Technology and information resources protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Technology and information resources 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.

Copyrights
In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from any technology resources must be used in conformance with applicable copyright and other law.

Copied material must be properly attributed. Plagiarism of information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Integrity of Information Resources
Information technology users must respect the integrity of computer-based information resources.

In making acceptable use of resources you are expected to:

- use resources only for purposes authorized by this procedure;
- protect your user ID, password, and resources from unauthorized use;
- access only information that is your own, that is publicly available, or to which you have been given authorized access;
- be aware of copyright laws as they apply to computer software and other materials that you may access with District information technology resources.

Unacceptable use of resources may include but is not limited to:

- unauthorized use of another person's system access, user ID, password, files, or data, or giving the use of one's system, user ID, password to another individual or organization;
- attempt to disguise the identity of the account or computer you are using;
- attempt to gain unauthorized access to resources and data, including other's passwords;
- attempt to circumvent, subvert, or disable system or network security measures;
- engaging in activities that may lead to disrupting services;
- intentionally damage files or make unauthorized modifications to District data;
- download, make or use illegal copies of copyrighted materials, software, or music, store such copies on District resources, or transmit them over District networks;
- creation or display of threatening, obscene, racist, sexist, defamatory, or harassing material which is in violation of existing law or District policy;
- use of the District's resources or networks for personal profit;
- installation of unauthorized hardware or software onto any District owned computer/network (the Information Technology Department or appropriate District authorized personnel is responsible for all installations, requests for exceptions should be sent to the Chief Information Officer);
- connect a personal computer to the District's network unless it meets technical and security standards established by the District.

Password Protection
An information technology 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. Users are required to change passwords as mandated by the District.

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

Disclosure

No Expectation of Privacy - All information stored on District technology resources is subject to subpoenas and local, state, and federal laws and regulations.

Dissemination and User Acknowledgment

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

Also see BP/AP 2510 titled Participation in Local Decision Making, BP/AP 4030 titled Academic Freedom, AP 6365 titled Accessibility of Information Technology, BP/AP 6520 titled Security for District Property, AP 6535 titled Use of District Equipment, and BP/AP 6700 titled Civic Center and Other Facilities Use

Office of Primary Responsibility: College Operations

Date Approved: February 17, 2009
(Replaces College of Marin Procedures 7.0020 DP.1 and 7.0032 DP.1)

Date Revised: June 28, 2011