General Institution

AP 3720 INFORMATION TECHNOLOGY USE

References:

15 U.S. Code Section 6801 et seq.;
17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1 subdivision (b);
16 Code of Federal Regulations Parts 314.1 et seq.;
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 hardware devices, software applications and services, licenses, 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. These technology resources are 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 hardware devices and associated peripherals, software and information resources, 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, 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 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 – Information technology users must respect copyrights and licenses to software and other online information.

Copying – Software, 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.

Protected software, 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.

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 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.

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; 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.

Additional 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.

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 - 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.

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 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 individual's (student, faculty, or staff) 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 local, state, federal, 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. 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.

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 Marin Community College District network and computer resources which discriminates against any person on the basis of national origin, religion, age, family and medical care leave, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, sex (which includes pregnancy, childbirth, breastfeeding and medical conditions related to pregnancy, childbirth), military and veteran status or because he/she/they is perceived to have one or more of the foregoing characteristics, or based on 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.

Disclosure: 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.

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

Offices of Primary Responsibility: Administrative Services, Information Technology

---

Date Approved: February 17, 2009 *(Replaced College of Marin Procedures 7.0020 DP.1 and 7.0032 DP.1)*
Date Revised: June 28, 2011
Date Revised: April 19, 2022