AP 3720 INFORMATION TECHNOLOGY 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 Information Resources are the sole property of West Valley-Mission Community College District. They may not be used by any person without the proper authorization of the District. The Information Resources systems 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 non-District owned devices whenever such devices are connected to District networks or information resources, regardless of whether used for administration, research, teaching or other purposes. This procedure includes all electronic devices, wired and wireless, that are used to gain access to the District 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 state and federal laws, collective bargaining contracts, and student code of conduct. 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; and/or civil or criminal legal action.

Copyrights and Licenses

Information Technology users must respect copyrights and licenses to software and other on-line 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.

Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users within the District or any portion of the District not exceed the number of original copies or otherwise legally acquired by the District or any portion of the District 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.

Fair Use - Fair use explicitly allows use of copyrighted materials for educational purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Rather than listing exact limits of fair use, copyright law provides four standards for determination of the fair use exemption:

- Purpose of use: Copying and using selected parts of copyrighted works for specific educational purposes qualifies as fair use, especially if the copies are made spontaneously, are used temporarily, and are not part of an anthology.

- Nature of the work: For copying paragraphs from a copyrighted source, fair use easily applies. For copying a chapter, fair use may be questionable.

- Proportion/extent of the material used: Duplicating excerpts that are short in relation to the entire copyrighted work or segments that do not reflect the "essence" of the work is usually considered fair use.

- The effect on marketability: If there will be no reduction in sales because of copying or distribution, the fair use exemption is likely to apply.

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

In making acceptable use of resources users 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.

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

- Attempt to circumvent, subvert, or disable system or network security measures;
- Engage 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 Systems Department or appropriate District authorized personnel is responsible for all installations, requests for exceptions should be sent to the Director of Information Systems).

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

Unauthorized Use - Technology users must not interfere with others access and use of the District information resources. 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 data storage systems and structures; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing and telecommunication facilities, equipment, software or computer files.

Unauthorized Programs - Technology users must not intentionally develop or use programs which disrupt other technology users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Technology 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
Technology users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Password Protection - An information technology user who has been authorized to use a password- protected account on District systems or controlled by the District on other systems 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.

Unauthorized Access includes, 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;

Abuse of Computing Privileges - Users of District information resources must not access information technology equipment and resources or networks without proper authorization, or intentionally enable others to do so, regardless of whether the information technology equipment and resources, 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
A technology user users must respect the rights of other technology 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).

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 and the system administrator.

Rights of Individuals - Users must not release any individual's (student, faculty, and 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 federal, state, or other applicable laws.

Personal Use - District information resources should not be used for personal activities not related to appropriate 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 appropriate within those domains.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of West Valley-Mission Community College District information technology equipment and resources, or network which discriminates against any person on the basis of national origin, religion, age, sex or gender, race, color, medical condition, ancestry, sexual orientation, marital status, physical or mental disability, 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 information 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 information resources 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 information 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 and computer 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.

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 acknowledgment and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:

Computer and Network Use Agreement

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 and/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 and/or Federal law.

Date Approved: January 18, 2012

*(This is **new** procedural language recommended by the Policy and Procedure Service)*