ACCEPTABLE TECHNOLOGY USE POLICY

The District recognizes that it offers a variety of instructional and administrative technology resources to support learning, enhance instruction, carry out the legitimate business of the District and provide the ability to communicate with other users worldwide. These resources are provided to the District's students and employees solely to support the District's mission and institutional goals, and use of these resources shall be consistent with the mission, goals and this policy. Such open access is a privilege, and requires that individual users act responsibly and ethically. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, policies and contractual obligations. These information resources and users' accounts are property of the District, whether accessed directly or remotely, and shall be maintained and upgraded according to District standards.

All existing laws (federal and state) and District and college regulations and policies apply, including not only those laws and regulations that are specific to computers, voice mail and networks, but also those that may apply generally to personal conduct.

Users may be held accountable for their conduct under any applicable college or District policies, procedures, or collective bargaining agreements. Improper use of technology resources may result in the loss of technology privileges throughout the District. Additionally, improper use can be prosecuted under applicable statutes. Complaints alleging improper use of District technology resources will be directed to those responsible for taking appropriate disciplinary action as specified under ENFORCEMENT below. Illegal reproduction of software protected by U.S. copyright law is subject to civil damages and criminal penalties including fines and imprisonment. The District is not responsible for any unlicensed software loaded on a computer by individual students or employees.

Each employee user will have his/her own login name and password. This password must be kept secure, meaning it should not be shared or posted anywhere. Employee users should only use their own login names and passwords.

The District's technology resources and all users' accounts are the property of the District. There is no right to privacy in the use of the technology resources or users' accounts, and the District reserves the right to monitor and access information on the system and in users' accounts for the purpose of determining whether a violation of this policy or Business Procedure 10.06 has occurred. The District will remove any information on the system which it determines to be in violation of this policy, or Business Procedure 10.06. User files[1] may be subject to search if such files are suspected of containing information that could be used as evidence in a court of law. In addition, systems administrators have the right to access user files as required to protect the integrity of the District systems or if they have a reasonable belief that there has been a violation of law or District policy by the user.

Users are reminded that e-mail and voice mail messages are files which are backed up as part of regular network operation. As such, deletion of messages does not remove all traces of the message. The District has taken reasonable steps to ensure privacy of e-mail and voice mail, but does not guarantee that privacy. The District is not liable for lost or deleted e-mail or voice mail. The sending of chain e-mail messages or excessive amounts of e-mail or voice mail is prohibited. E-mail or voice mail used for harassment, gain, commercial purposes or for promoting personal views is strictly prohibited.

1. Files include e-mail, voice mail, documents and records.

(over)

When accessing remote resources from District facilities, users are responsible for obeying the policies and administrative regulations of the District and the policies of the other organizations in the same manner as they would if they were accessing the District's resources from District-owned resources.

No person utilizing District technology resources will disclose or disseminate personal information concerning students attending the District's schools. Student files, as kept on District technology resources, are considered educational records as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232 (g) of the United States Code, also referred to as the Buckley Amendment).

The Chancellor or his/her designee is hereby authorized to adopt and implement such administrative procedures as are necessary and appropriate to implement this policy.

ENFORCEMENT

All District resources must be properly labeled with a District asset tag. Any resource bearing a District asset tag is considered to be covered by this policy. In addition, this policy must be made available in all student computing environments and provided to employees at hiring.

Penalties may be imposed under one or more of the following: CCCCD and individual college regulations, discipline up to and including termination, California law, and the laws of the United States.

Minor infractions of this policy, when likely accidental in nature, (e.g., poorly chosen passwords) are typically handled internally in an informal manner by electronic mail or in-person discussions.

More serious or repeated violations may result in disciplinary action including, but not limited to, the temporary or permanent loss or modification of technology resource access privileges, as well as notification of a student's instructors/counselor, department/division chairs, and/or the dean of students, or the department chair or manager in the case of an employee.

Offenses which are in violation of local, state or federal laws will result in the immediate loss of all technology resource privileges, and will be reported to the appropriate college and law enforcement authorities. The District may use monitoring technologies to assure that all activities support the District's mission and institutional goals and policies and are not in violation of local, state or federal laws.

The District will be responsible for bringing into compliance all listed, unlicensed, job-required software.

Historical Annotation:
BP4007: Adopted 4/30/97
BP5030: Revised 1/30/02
Revised 12/8/10

Related Board Policies:
Board Policies 4003, 4006

Related Procedures:
Business Procedure 10.06
Curriculum and Instruction Procedure 4003
Human Resources Procedure 1040.01

Related Implementation Guideline:
Implementation Guideline 2012.01