



Individual departments/units within the District may define additional conditions of use for information resources under their control. These conditions must be consistent with this overall regulation but may provide additional detail, guidelines and/or restrictions. These guidelines can cover such issues as allowable connect time and disk space, handling of irretrievable mail, responsibility for account approval, and other items related to administering the system.

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. All access to the District's computer resources, including the issuing of passwords, must be approved by a designee of the District.

Computer users of the District's 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. 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 computer privileges.

6006.5

The Vice Presidents shall be responsible for the overall coordination and implementation of regulations relating to the use of technology. Managers, department heads, and/or Deans/Directors will take an active role in assuring that technology users are familiar with these regulations. Computer users must respect the integrity of computer-based information resources.

- A. Illegal copies of copyrighted programs may not be made or used on school equipment.
- B. It is not an infringement for the owner of a copy of a computer software program to make or authorize the making of another copy or adaptation of that computer software program provided:
  - 1. that such a new copy or adaptation is created as an essential step in the utilization of the computer software program in conjunction with a computer and that it is used in no other manner, or
  - 2. that such a new copy is a backup copy and that all such copies are destroyed in the event that the original copy of the computer software program is no longer in the possession of the registered owner.

These guidelines are based on Public Law 96-517, Section 7(b) which amends Section 117 or Title 17, or subsequent laws, of the United States Code.

Computer users must not interfere with the access and use of the District's computers by other computer users. 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.

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 programs will result in disciplinary action as provided in this regulation, and may further lead to civil or criminal legal proceedings.

Defects (e.g. "loopholes") in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given. Any defects discovered in system accounting or system security must be reported immediately to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

6006.6

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to any system or to another person's information are a violation of District policy and may violate federal, state and local laws.

Unlawful Messages – Computer 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.

Information Belonging to Others – Computer 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 – Computer users must not release any individual’s (student, faculty or staff) personal information to anyone without proper authorization.

User Identification – Computer 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 and technology resources should not be used for partisan political activities where prohibited by federal, state or other applicable laws.

Personal Use – District information and technology resources should not be used for personal activities unrelated to appropriate District functions, except in a purely incidental manner.

Commercial Use – District information and technology resources should not be used for commercial purposes. Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions. Computer users are reminded that the “.cc” and “.edu” domains on the internet have rules restricting or prohibiting commercial use, and users may only conduct activities that are appropriate within those domains.

6006.7 All computer 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 on the basis of race, religious creed, color, national origin, ancestry, gender, sexual orientation, age (over 40), disability, marital status, medical condition or disability or obligations to the National Guard or Reserve Forces of the United States.

No computer user shall use the District’s network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District policy or regulation regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

6006.8 Computer users are responsible for maintaining the following items:

- A. An environment in which access to all District computing resources are shared equitably among users. The system administrator of each system sets minimum guidelines within which users must conduct their activities.
- B. An environment conducive to learning:
  - 1. A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that the District's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by the District.
  - 2. Many of the District computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin board, conferences, etc. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that the District does not assume responsibility for the contents of any of these outside networks.
  - 3. The user agrees never to attempt to transmit or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not the District, which is acting solely as the information carrier.
- C. An environment free of illegal or malicious acts.
- D. The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which a user is authorized, or any attempt to deprive other authorized users of resources or access to any District computer system shall be regarded as malicious, and may be treated as an illegal act.
- E. Users are responsible for backup of their own data.

6006.9 An account assigned to an individual must not be used by others without written permissions from the Deputy Director for Network Services. The assigned individual is responsible for the proper use of the account including proper password protection.

6006.10 Software installation, copies, licenses and ownership:

- A. Computer users must respect copyrights and licenses to software and other on-line 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 the 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.

- B. Only legally purchased software may be used on District-purchased computers. Information systems designated personnel will install District-purchased software on computers provided for faculty and staff use. To prove legal ownership and compliance with copyright restrictions, a copy of the license for faculty-owned or staff-owned software must be sent to IITS.
- C. Departments which have purchased software under a site license agreement must have the license agreement available on site to prove legal ownership and compliance with copyright restrictions or have sent a copy of the license agreement to IITS.

6006.11 Any person detecting the apparent illegal use of software will report the suspected usage to the Associate Vice President of Instructional and Information Technology. The Associate Vice President of Instructional and Information Technology, after ascertaining the extent of such use, will meet with the appropriate dean or manager to discuss how any needed software

can be legally purchased or licensed and the disposition of any illegal software.

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies and regulations. Such suspected violation will be confidentially reported to the violator's immediate supervisor.

6006.12

The District reserves the right to monitor all use of District computer, telecommunications, and classroom technology resources to assure compliance with these regulations. Users should be aware that they have no expectation of privacy in the use of the District's computer, telecommunications, and classroom technology resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this regulation and the integrity and security of the systems.

Users must be aware of the possibility of unintended disclosure of communications.

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.

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 computers must be disclosed if requested by a member of the public.

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

Dissemination and User Acknowledgement – All users shall be provided copies of these regulations and be directed to familiarize themselves with them. An on-screen message addressing these regulations shall be displayed on District user systems. The message screen shall appear as part of accessing the District network. This message screen acknowledgment shall be in the form as follows:

Computer, Telecommunications and Classroom Technology Use Agreement

I agree to abide by the standards set in Policy 6006 and Administrative Regulations 6006 for the duration of my employment and/or enrollment. I am aware that violations of the policy or administrative regulations may subject me to disciplinary action, including but not limited to revocation of

my network access and up to and including prosecution for violation of State, Federal or local law.

6006.13 Appropriate regulations regarding student access to and use of computer, telecommunications, and classroom technology shall be developed, consistent with this policy and administrative regulations, approved by the appropriate vice president or designee and posted in prominent locations within all student-access computer areas and other appropriate locations throughout the college. These regulations shall be reviewed periodically and revised as needed.

Adopted: November 17, 1997

Revised: May 24, 2011