AP 3720 Computer and Network Use

Reference:

Education Code Section 70902; Copyright Act (17 U.S.C. § 101 et. seq.; Penal Code § 502

The District's computers and network systems (computing resources) are the sole property of the Feather River Community College District. They may not be used by any person without the proper authorization of the District. Computing resources are to be used for District instructional and work related purposes only, except as noted in the Personal Use clause of the Usage section.

This procedure applies to all District students, faculty, administrators and staff and to all others granted use of District computing resources. This procedure refers to all District computing resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and information technology resources owned, leased, operated, or contracted by the District. This includes desktop and laptop computers, printers, monitors, servers, routers, hubs, removable storage devices, switches, scanners, mobile computing equipment, software, and all other information technology resources, regardless of whether they are used for administration, teaching or other purposes.

Legal Process

This procedure exists within the framework of the District's Board Policy BP3720 and all applicable state and federal laws. A user of District computing resources who is found to have violated any of these procedures may be subject to progressive disciplinary action, including but not limited to revocation of their network account, disciplinary suspension or expulsion from the College or termination from employment and/or civil or criminal prosecution.

Copyrights and Licenses

All computer users must abide by copyrights and license terms for software and other computer-based 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, including but not limited to commercial, shareware, and freeware may not be copied into or from any District computer or other computing resource, except pursuant to a valid license or as otherwise permitted by copyright law. The Information Services Department staff are the only District employees authorized to install, upgrade or modify software.

- Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users does not

exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract or license terms.

- Copyrights - In addition to software, all other copyrighted information (text, images, icons, audio materials, etc.) retrieved from computers or computing resources must be used in conformance with applicable copyright and all other relevant laws. Copied material must be properly attributed. Plagiarism of computer-based information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Integrity of Computing Resources
Computer users must respect the integrity of all computer-based information resources.

- Modification or Removal of Equipment - Computer users must not attempt to modify, disconnect, or remove computer equipment, software, or other computing resources.

- Unauthorized Use - Computer users must not interfere with other user's ability to use the District's computing 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 computing resources, equipment, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing resources, including, but not limited to equipment, software or computer files.

- Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of any computing resource, or which damage the software or hardware components of any computing resource. Computer users must ensure that they do not use utilities or programs, that interfere with other computer users or that modify normally protected or restricted portions of any computing resource or other user's accounts. The use of any unauthorized program, including data encryption programs, may result in progressive disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access
Computer users may only access computers and other computing resources to which they are legitimately entitled. They must not seek to gain access to non-authorized computing resources and must not assist others in gaining unauthorized access to District computers or computing resources.

- Abuse of Computing Privileges - Users of District computing resources must not access computers, computer software, computer files, or networks without

proper authorization, or intentionally enable others to do so, regardless of whether the computer, computer software, computer files, or network in question is owned by the District. Student network accounts must not be used to access office computers under any circumstance. Abuse of the networks to which the District belongs will be treated as an abuse of District computing resources.

- Reporting Problems - Any problems discovered with network performance or computer security must be reported promptly to the Information Services Department staff so that steps can be taken to investigate and resolve the problem. The same is true if you suspect your network account has been compromised in any way.

- Password Protection - No sharing of passwords to access District computing resources is allowed. Computer users are responsible to make sure that others do not use their network account or passwords for any reason. A password-protected screen saver is required on all office computers to minimize the risk that an unattended computer is used for unauthorized access to the network or other computing resources. A computer user who has been authorized to use a password-protected program or other computing resource may be subject to both civil and criminal liability if the user discloses the password or makes the computing resource available to others.

Usage

Computer users must respect the rights of other computer users. Attempts to circumvent security mechanisms in order to gain unauthorized access to the network or to another person's information, or subvert computer or network security measures are a violation of District procedures and may also violate applicable law. Any activity that may negatively impact the operation of the network is prohibited and may be enforced by blocking particular web sites or Internet protocols. Users are responsible for all activities originating from their network accounts.

- 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 laws or any District policy, or which constitute the unauthorized release of confidential information. Access to various email and other communication systems and distribution lists may be restricted.

- Commercial Use - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions. Some District organizations may be authorized to sell items, according to the stated purpose of the organization(s). District computing resources must not be used by individuals for commercial purposes. Users also are reminded that ".edu" domains on the Internet have rules restricting or prohibiting commercial

use, and users may not conduct activities not appropriate within those Internet domains.

- Information Belonging to Others - Users must not intentionally seek to obtain copies of computer-based information, or modify data files, programs, or passwords belonging to other users.

- Rights of Individuals - Users must not release any individual's (students, faculty, administrators or staff) confidential information to anyone without proper authorization. No confidential information is to be stored on any District owned mobile computing device or removable storage media, including notebook computers, PDA devices, cellular phones, diskettes, CD/DVD discs, or USB flash drives.

- User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account or computer workstation.

- Political Use - The District is a public, 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, therefore the District's computing resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws.

- Personal Use - District computing resources must not be used for personal activities not related to appropriate District functions, except in a purely incidental manner. The appropriate administrator or supervisor will typically handle minor infractions of this section by District employees informally. The Chief Student Services Officer informally handles minor infractions by students.

Nondiscrimination
All users have the right to be free from any conduct connected with the use of the District's network and computing resources that discriminates against any person. No user shall use the District's network and computing resources to transmit any message, create any communication of any kind, or store information in any form which violates any District procedure or applicable law regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure
The District reserves the right to monitor all use of the District's network and computing resources to assure compliance with these procedures. Users should be aware that they have no expectation of privacy in the use of the District's network and computing resources. The District will exercise this right only for legitimate District purposes,

including but not limited to ensuring the integrity, performance, and security of its computing resources.

- Possibility of Disclosure - Users should be aware of the possibility of unintended disclosure of electronic communications and other digital information stored on the District's computers or computing resources.

- Retrieval - It is possible for information entered into 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's network and computers must be disclosed if requested by a member of the public.

- Litigation - Computer transmissions may be discoverable in litigation.

Dissemination And User Acknowledgment
All users shall be provided with printed copies of these procedures and be directed to familiarize themselves with them.

Users shall sign and date the acknowledgment included in this procedure stating that they have read and understand these procedures, and will comply with them. This acknowledgment shall be in the form as follows:

Computer and Network Use Agreement

I have received a copy of the District's Computer and Network Use Procedure (AP3270) dated April 12, 2006, and this Agreement. My signature below certifies that I have read and understand the guidelines for computer and network use. I agree to abide by the requirements stated in AP3270 for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Network Use Procedure may subject me to progressive disciplinary action, including but not limited to revocation of my network account, disciplinary suspension or expulsion from the College or termination from employment and/or civil or criminal prosecution.

Reference: BP #3715
Approvals:
Cabinet: April 24, 2006