AP 3720 Computer Use – Computer and Electronic Communication Systems

Contents

Computer and Electronic Communication Systems

1.0 Introduction

This procedure applies to all district students, faculty and staff and to others granted use of District computer and electronic communication systems. This procedure applies to all computer and electronic communication systems, either District owned or individually owned which interfere with District operations or through operation violate District policy. For purposes of this procedure, Computer and Electronic Communication Systems include, but are not limited to, electronic mail, Internet and intranet services, voice mail, audio and video communications and facsimile messages which are provided using District-owned, leased, or rented computer hardware, software, databases and telecommunications systems. Campus*(*es*)* may adopt acceptable use procedures which are not in conflict with this procedure.

1.1 Academic Freedom:

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The freedom to teach and learn depends upon appropriate opportunities and conditions not only in the classroom, but on the campus as a whole. The responsibility to secure and to respect general conditions conducive to academic freedom is shared by all members of the academic community -- faculty, staff, and students. Nothing in this policy limits or removes the right of free speech or the academic freedom of faculty, staff and students engaged in the learning process.

This computer use policy seeks to achieve objectives necessary for the legitimate and proper use of the VVC computing resources. It is intended that these ends should be achieved in ways that respect the legitimate interests and rights of all computer users.

AP 3720 Computer Use – Computer and Electronic Communication Systems

Nothing in this procedure shall be interpreted to expand, diminish or alter academic freedom, articulated under Board Policy 4030 Administrative Procedure 4030 or any collective bargaining agreements. System and network administrators are expected to respect the college academic freedom policies.

2.0 Access to Systems

2.1 District computer and electronic communication systems components, devices, and services are District property. Any electronic device, mail address, account, or license associated with the District or assigned by the District to individuals or functions of the District are the property of the District. All electronic devices, mail addresses, accounts, and licenses and all devices connected to the District's secured computer and electronic communication systems must meet District interface and security protocol as determined by the District. For purposes of this procedure, the word "secured" means protection of District systems and data from unauthorized use.

2.2 Access to the District's computer and electronic communications systems is a privilege that may be revoked or restricted by the Superintendent/President or designee at any time without prior notice and without the consent of the user. Some reasons for revocation or restriction of access to services include, but are not limited to, the following:

2.2.1 when required by and consistent with law, or when there is probable cause to believe that violations of policy or law have occurred;

2.2.2 when necessary to prevent loss of evidence of violations of policy or law;

2.2.3 when necessary to prevent property damage or loss of property, or bodily harm;

2.2.4 when necessary to prevent liability to the District;

2.2.5 when business operational needs warrant, as determined by the Superintendent/President or designee.

AP 3720 Computer Use – Computer and Electronic Communication Systems

2.3 Computer and electronic communications systems access privileges granted to users on the basis of individually-assigned accounts which use passwords may not be transferred, shared, or converted to other individuals without explicit permission from the District.

2.4 Voice mail means an audio message transmitted telephonically between two or more telephones, whether or not the message is converted to hard copy format after receipt and whether or not the message is heard upon transmission or stored for later retrieval. Voice mail includes telephonic messages that are transmitted through a local, regional, or global telephone network.

3.0 Privacy Disclosure and Use Disclaimer

3.1 District Electronic Communication Systems and services are District property. Any electronic mail address or account associated with the District, or any sub-unit of the District, assigned by the District to individuals, sub-units, or functions of the District, is the property of the District. Users should be aware that because of the nature of electronic communications and the public character of the District's business, the District's computer and electronic communication systems are not private. Routine maintenance and system administration may result in observation of the contents of files and communications. Access to District computer and electronic communication systems may be logged at the discretion of the District. Users should be aware that there is no expectation of privacy or confidentiality in the content of electronic communications or computer files sent and received on the District's systems or stored in the users' directories, and therefore, users should exercise extreme caution in using electronic communications to communicate or store information of a confidential or sensitive nature. Portable devices without encryption such as laptop computers and data storage devices are especially susceptible to theft or loss and should not be used to store confidential information.

3.2 Electronic communications that utilize district computer and electronic communication systems equipment, including communication records arising from personal use, whether or not created or stored on District equipment, may be presumed to constitute a District record subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. Also, it is possible for information entered on or transmitted via computer and electronic communication systems to be retrieved, even if a user has deleted such information. Users should be aware of the implications of this presumption in any decision to use district

computer and electronic communication systems for personal use.

3.3 Although the District respects the privacy of users and does not routinely inspect, monitor, or disclose electronic communications, the District reserves the right to inspect, monitor, or disclose electronic communications at any time without prior notice and without the consent of the user as directed by the Superintendent/President or designee. Reasons for inspecting, monitoring or disclosing electronic communications include, but are not limited to, the following

3.3.1 when required by and consistent with law, or when there is probable cause to believe that violations of District policy or law have occurred;

3.3.2 when necessary to prevent loss of evidence of violations of District policy or law;

3.3.3 when necessary to prevent property damage, loss, or bodily harm;

3.3.4 when necessary to prevent liability to the District.

3.4 Inspection or monitoring, other than for routine maintenance and system administration, must be authorized by the Superintendent/President or designee. Such inspection or monitoring must be limited to materials related to the investigation, and the confidentiality of the inspection must be maintained to the highest degree possible. In the event a search of an employee's computer files is authorized, a reasonable effort must be made to secure technical assistance from a person designated by the constituent group and/or union of the employee whose files are being searched.

3.5 The District will make every possible effort, but cannot guarantee the protection of users from receiving electronic communications they may find offensive, nor can the District guarantee the authenticity of electronic communications received, or that electronic communications received were in fact sent by the purported sender. Users are responsible for materials they access and disseminate on the District's computer and electronic communication systems.

AP 3720 Computer Use – Computer and Electronic Communication Systems

3.6 The District will make every possible effort to protect District data integrity, but assumes no responsibility for the loss of data on district owned Computer and Electronic Communication Systems due to computer viruses or other destructive software, activities as a result of flaws in the application or operating system software. This includes phishing and ransomware attacks.

4.0 Acceptable Use

4.1 The District's computer and electronic communication systems are provided to support the educational mission of the college and the administrative functions that support this mission, and are to be used primarily for District business-related purposes. Consistent with this purpose, these procedures are not intended to inhibit academic freedom or the acquisition of information. Incidental personal use is permitted, provided that such incidental personal use conforms to this procedure and such use does not:

4.1.1 Interfere with the user's employment or ability to perform work assignments or those of another employee;

4.1.2 Directly or indirectly interfere with the District's operation of computer and electronic communication systems;

4.1.3 Burden the District with noticeable incremental cost.

4.2 Use of the District's computer and electronic communication systems and services is limited to the District's students, faculty, staff and other authorized persons. Users of the District's computer and electronic communication systems and services are expected to do so responsibly and in compliance with local, state, and federal laws, as well as the policies and procedures of the District, and with normal standards of professional and personal courtesy and conduct.

5.0 Unacceptable Use

5.1 The use of the District's computer and electronic communications systems for any of the following is prohibited:

AP 3720 Computer Use – Computer and Electronic Communication Systems

5.1.1 Use which violates local, state or federal law;

5.1.2 Use which violates District policies or administrative procedures;

5.1.3 Use which violates District software licensing agreements, use of software without legal authorization, or unauthorized duplication, transmission, or use of unlicensed copies;

5.1.4 Use for private commercial purposes not under the auspices of the District;

5.1.5 Use for personal financial gain;

5.1.6 Use of District computer and electronic communications systems including, but not limited to, the following:

5.1.6.1 Knowingly loading viruses onto or from any computer connected to the district's system;

5.1.6.2 Attempting or gaining unauthorized access to, or alteration of data, files, emails or passwords (hacking);

5.1.6.3 Unauthorized tampering with computing resources, including connecting or disconnecting computer equipment or otherwise altering the set-up of any computer or network of computers;

5.1.6.4 Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technologies Department is made.

5.1.6.5 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

5.1.6.6 Circumventing user authentication or security of any host, network or account.

AP 3720 Computer Use – Computer and Electronic Communication Systems

5.1.6.7 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet

5.1.6.8 Engaging in any activity that inappropriately restricts or inhibits any other user from using or enjoying the VVC network, including "hacking", "cracking", "spoofing", or defacing any portions of the VVC network, including any VVC websites.

5.1.6.9 Launching or facilitating a denial of service attack (DoS) from or on the VVC Network.

5.1.6.10 Using the VVC network in connection with illegal or unlawful file sharing.

5.1.6.11 Using the VVC network to operate a general-purpose proxy or "open proxy" service.

5.1.6.12 Using the VVC network as a "miner" or "forger" of BitCoin or other cryptocurrencies.

5.2 Use of District computer and electronic communications systems including, but not limited to, the following is strictly prohibited:

5.2.1 Use for unauthorized advertising, campaigning, soliciting or proselytizing for any religious or political cause, outside organization, business, or individual;

5.2.2 Use for intentionally sending or accessing pornography or obscene materials other than for authorized research or instructional purposes;

5.2.3 Use for sending defamatory, intimidating, threatening, harassing, discriminatory, abusive or patently offensive material to or about others, or any use that violates the District policies regarding unlawful discrimination;

5.2.4 Use that violates District policy regarding intellectual property

AP 3720 Computer Use – Computer and Electronic Communication Systems

5.2.5 Use for unlicensed downloading, copying, or distributing of copyrighted work(s) such as movies or music for other than legally authorized uses, or uses authorized by the District.

5.2.6 Use for connection of non-district devices to the District's computer and electronic communications systems that results in a violation of this policy;

5.3 Users of the District's computer and electronic communication systems shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the District unless authorized to do so. Where appropriate, an explicit disclaimer shall be included.

5.4 Users of the District's computer and electronic communication systems shall not employ a false identity or otherwise transmit or attempt to transmit any message which is misleading as to origination.

5.4.1 Posting, distributing or transmitting chain letters, mass mailings, spam mail, any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index or "data mine

5.4.2 Unauthorized use, or forging, of e-mail header information

6.0 District Access and Disclosure

Violations of District policies and procedures governing the use of District computer and electronic communication systems may result in the restriction of access to District computer and electronic communication systems and appropriate disciplinary action, up to and including dismissal.

6.1 Users should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the District's computer and electronic communication systems or stored in the users' directory.

AP 3720 Computer Use – Computer and Electronic Communication Systems

6.2 Although the District does not routinely inspect, monitor, or disclose electronic communications, the District reserves the right to inspect, monitor, or disclose electronic communications without prior notice and without consent. Such inspections must be authorized by the Superintendent/President, or designee. Reasons for inspecting, monitoring or disclosing electronic communications include, but are not limited to, the following: when required by and consistent with law; when there is significant reason to believe that violations of policy or law have occurred; when failure to act may result in significant bodily harm, when significant property loss or damage would result, when loss of significant evidence of one or more violations of law or of District policies would result, when significant liability to the District or to members of the District community would result; or significant liability to business purposes, such as inspection of the contents of electronic messages in the course of an investigation triggered by indications of misconduct. The inspection must be limited to materials related to the investigation and the confidentiality of the inspection must be maintained to the highest degree possible. In the event a search of an employee's computer files is authorized, a reasonable effort must be made to secure technical assistance from a person designated by the constituent group and/or union of the employee whose files and/or systems are being searched.

7.0 Computer and Electronic System Agreement

As a condition of providing access to the District's computer and electronic communications systems, users shall sign an agreement, in a form prescribed by the Superintendent/President, acknowledging that the user has read and understands the provisions of this procedure and agrees to comply with the terms stated herein.

References:

15 U.S. Code Sections 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, 45

AP 3720 Computer Use – Computer and Electronic Communication Systems

Computer and Electronic Communication Systems Use Agreement

I have been provided with, and have read District Administrative Procedure 3720, Computer Use - Computer and Electronic Communications Systems. I agree to comply with the provisions of Administrative Procedure 3720 regarding the use of the District's Computer Use - Computer and Electronic Communication Systems procedure.

_____ _____

Signature Printed Name