AP 3720 Computer and Electronic Communication Systems

Reference:

Education Code Section 70902;
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

1.0 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, technology endpoints, electronic communication and collaboration systems, software, data, and intellectual property which traverse District-owned, leased, or rented computer hardware, software, database and communication and collaboration systems. Campuses may adopt acceptable use procedures which are not in conflict with this procedure.

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 Chancellor 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 District.

AP 3720 Computer and Electronic Communication Systems

2.3 Computer and electronic communications systems access privileges will be granted to users only with individually-assigned accounts which must use strong passwords. 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 between two or more systems, whether or not the message is converted to digital 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 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. District computer and electronic systems may be subject to device location tracking. Users should be aware that there is no expectation of privacy or confidentiality in the content of electronic communications or data sent, received, or stored on District systems, 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 any District 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. 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. 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;

AP 3720 Computer and Electronic Communication Systems

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 Chancellor, Vice Chancellor, or President. 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.

3.5 The District cannot protect 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.

3.6 The District assumes no responsibility for the loss of data on individual owned or District-owned Computer and Electronic Communication Systems due to malicious or destructive software, or as a result of flaws in the application, operating system, or network.

4.0 **Acceptable Use**

4.1 The District's computer and electronic communication systems are provided to support the educational mission of the colleges, North Orange Continuing Education, and the administrative functions that support this mission, and are to be used primarily for District business-related purposes. 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.

4.2.1 Under no circumstance shall any employee access or alter their own personal records, or cause another employee to access or alter their

AP 3720 Computer and Electronic Communication Systems

personal records. Banner self-service and myGateway functions are permissible.

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

4.3.1 Use which violates local, state, or federal law;

4.3.2 Use which violates board policies or administrative procedures;

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

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

4.3.5 Use for personal financial gain;

4.3.6 Use, other than for purposes for an authorized course of instruction or system administration that interferes with, disrupts, causes excessive strain on, or interferes with others' use of District computer and electronic communications systems including, but not limited to, the following:

4.3.6.1 Knowingly loading malicious programs onto or from any computer systems;

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

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

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

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

4.3.9 Use that violates board policy regarding intellectual property;

4.3.10 Use for intentionally sending or accessing pornography or patently obscene material other than for authorized research or instructional purposes;

4.3.11 Use for unlicensed downloading, copying, or distributing of copyrighted works such as movies or music for other than legally authorized uses, or uses authorized by the District;

AP 3720 Computer and Electronic Communication Systems

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

4.3.13 Personal use inconsistent with section 4.3 of this procedure;

4.3.14 Personal use which processes, stores, or transmits credit card information.

4.4 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.

4.5 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.

4.6 The District encourages the use of electronic communication systems to conduct all communication with the community, students, faculty, staff, and business partners. Communication sent from the District or any representative acting on behalf of the District will exclusively use District provided systems. Electronic mail, facsimiles, text messages, or other data that originated or traversed District systems should not be forwarded to personal accounts while conducting District business.

5.0 **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.

5.1 Users should have no expectation of privacy or confidentiality in the content of electronic communications or other data sent, received, or stored on District computer systems.

5.2 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. 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. Such inspections must be authorized by the Chancellor, Vice Chancellor, or President. 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.

AP 3720 Computer and Electronic Communication Systems

6.0 **Information Security Compliance**: In accordance with the Gramm-Leach-Bliley Act for entities that participate in Title IV Educational Assistance Programs, the District will develop, implement, and maintain a comprehensive information security program containing administrative, technical, and physical safeguards.

6.1 The Vice Chancellor of Educational Services and Technology in collaboration with the District Director, IT Infrastructure & Operations and District Director, Enterprise IT Applications Support & Development are responsible for coordinating the District information security program.

6.2 The District shall conduct an information security risk assessment to identify internal and external risks to the security, confidentiality, and integrity of student or District information. Risks will be assessed in each of the following areas on an annual basis:

6.2.1 Employee training and management;

6.2.2 Information systems, including network and software design, as well as information processing, storage, transmission and disposal;

6.2.3 Detecting, preventing and responding to attacks, intrusions, or other systems failures

6.3 Based on the results of the information security risk assessment, the District shall implement appropriate information safeguards to control the risks identified and regularly monitor the effectiveness of the safeguard's controls, systems, and procedures.

6.4 The District will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the District information at issue; and require service providers by contract to implement and maintain such safeguards.

6.5 The District will evaluate and adjust the information security program in light of the results of the testing and monitoring required; any material changes to the District's operations or business arrangements; or any other circumstances that may have a material impact on the information security program.

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 Chancellor, acknowledging that the user has read and understands the provisions of this procedure and agrees to comply with the terms stated herein.

See Board Policy 3720, Computer and Electronic Communication Systems and Administrative Procedure 6365, Accessibility of Information Technology.

Date of Adoption: March 23, 2004

AP 3720 Computer and Electronic Communication Systems

Date of Last Revision: January 25, 2021 District Consultation Council
April 27, 2020 District Consultation Council
September 25, 2017 District Consultation Council
September 26, 2016 District Consultation Council
November 23, 2015 District Consultation Council
April 28, 2008 Chancellor's Cabinet

AP 3720 Computer and Electronic Communication Systems

Computer and Electronic Communication Systems Use Agreement

I have been provided with, and have read District Administrative Procedure (AP) 3720, Computer and Electronic Communications Systems. I agree to comply, and assist any staff for which I am responsible for to comply, with the provisions of AP 3720 regarding the use of the District's computer and electronic communications systems, and by any future terms and conditions of the procedure that may be developed.

I understand that District computer and electronic communications systems components, devices, and services are the property of the District and that access to the District's computer and electronic communications systems is a privilege that may be revoked or restricted at any time without prior notice and without consent of the user.

I also understand that because of the nature of electronic communications and the public character of the District's business, there is no expectation of privacy or confidentiality in the content of electronic communications or computer files sent and received on the District's computer or electronic communications systems or stored in the users' directories, and that 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.

_____

Signature