AP 3720 COMPUTER AND NETWORK USE

References:

Government Code, Section 3543.1(b);
Penal Code, Section 502;
15 U.S. Code Section 6801 et seq.;
17 U.S.C., Sections 101 et seq.;
Cal. Constitution Article 1, Section 1;
16 CFR Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, and 45

Preamble

These standards and administrative procedures defining and governing acceptable and unacceptable use will apply to anyone who uses any computer system, network system, Internet connectivity or intranet site or other data processing resources provided by the District. It is considered a violation of District policy to use the District's network and/or Internet access in such a way that it interferes with or is incompatible with the user's performance, duties, or responsibilities.

As a condition for receiving and exercising computing privileges, a user of District computing systems must read, understand, and comply with the standards and procedures outlined herein and to any further guidelines provided by the administrators of each area and/or system.

Unacceptable use is prohibited and can become grounds for loss of computing privileges, disciplinary action up to and including termination or expulsion and/or legal actions under local, state and federal laws.

The District is committed to providing access to computing resources to all members of its current student body, faculty, staff and members of the Board of Trustees and other authorized community members. While the fullest possible open access to District computing facilities and systems is consistent with the educational and service missions of the District, such access to this valuable and vulnerable District resource is a ***privilege***. The District is responsible for securing its network and computing systems to a reasonable degree against failure, loss of data, and unauthorized access, while making them accessible to the largest possible group of authorized and legitimate users and uses within the financial and educational constraints of the District.

Privileges

An individual user must respect the rights of other users, respect the integrity of the systems he/she/they is using, and observe all relevant laws and regulations.

Users do not own either District computers, accounts or network, but rather are granted the use of such computers, accounts and network. The District owns the computers, accounts and network and grants individuals the privilege of using them.

District employees may apply for user IDs to utilize email and restricted Internet services. Connectivity to the Internet from off-campus locations is not provided for by the District.

Responsibilities

Each user is held accountable for his/her/their actions while using District resources. By using his/her/their District provided resources, each user acknowledges and agrees to abide by and conform to the following:

- Computers and networks are provided to support District related research, instruction, learning, communication, distribution of scholarly information, and administrative activities.
- A user shall not attempt to modify any system or network or attempt to crash or "hack" into District systems. A user shall not tamper with any software protections or restrictions placed on computer applications or files to protect shared assets, assets managed by others, or software or data not part of a learning or research program in approved curriculum. Unless properly authorized, a user shall not attempt to access restricted portions of any operating system or security software. Improperly accessing or attempting to access confidential information concerning students or employees is prohibited. A user shall not attempt to remove existing software or add his/her/their personal software to District computers and systems unless authorized by the Director of Information Technology or his/her/their designee.
- Prior to the adoption or approval of District-acquired curriculum and other electronic and information technology, the authorizing Dean/area manager shall contact the Information Technology Department or the Purchasing Department to ensure that the proposed materials and/or technology meet or exceed the accessibility, licensing, and compatibility standards required by law, by Board Policy, and/or Administrative Procedure.
- An authorizing Dean/area manager must also contact the Information Technology Department to verify software accessibility for students with disabilities prior to the purchase and installation of any new software or hardware for educational programs.
- A user shall use only his/her/their designated computer account. An account is non-transferable: a user shall not use another individual's ID, password or account. A user should respect the privacy and personal rights of others and not access or copy another user's email, data or files without permission. A user is responsible for his/her/their own computer account(s) and shall not allow others to use his/her/their account(s). A user should take precautions, such as locking the computer on which he/she/they is working when he/she/they is not able to physically control access, so that others may not access his/her/their computer resources. A user should select a secure password, one that cannot be found within the dictionary, or easily guessed. The use of upper/lower case letters in conjunction with numbers in selecting a password is highly recommended.

- A user is responsible for using software and electronic materials in accordance with copyright and licensing restrictions and applicable District policies. Both District policies and the law expressly prohibit the copying of software in violation of their copyrights.

Individual User Rights

An authorized user is entitled to due process rights as described in Board Policies, Administrative Procedures and collective bargaining agreements.

The District will respect the exercise of academic freedom as described in Board Policy and an individual user's right to free speech provided that the exercise of such right does not violate any existing District Board Policy, Administrative Procedure, local, state or federal laws. Individual rights to free speech do not overrule or preclude the express prohibition of harassment of individuals on or off campus.

The District and its authorized users shall respect individual ownership rights to intellectual property, subject to existing District Board Policies, Administrative Procedures and collective bargaining agreements.

Virtually no online activities or services guarantee absolute privacy. It is impossible for the District to protect the privacy of email messages and other electronic files or documents. A user should be aware that electronic mail, documents and files are not entirely private and are more analogous to an open postcard than to a letter inside a sealed envelope traveling through the U.S. mail. A user should exercise appropriate care and caution.

The District cannot protect an individual against the receipt of material that may be offensive to him/her/them. A user of District electronic computing is warned that he/she/they may receive material that is offensive. Likewise, an individual who uses email or those who place personal information on the Internet should know that the District cannot protect an individual from an invasion of privacy. The District will make every reasonable attempt to honor the privacy of an individual using the District's computing resources for District business within the guidelines of the Electronic Communications Privacy Act (ECPA), which makes it illegal to intercept electronic communications on a public or private network without proper authorization, and state and federal students records laws including the Family Educational Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accountability Act (HIPAA).

The District reserves the right, for an extraordinary reason (e.g., basic system security, the safety of the campus or of an individual member of the campus community, the interception of suspected illegal, or inappropriate activity, etc.), to access and monitor all files, and Internet and email use.

Appropriate Uses of District Computer Resources

The District's computing facilities and network systems are provided to support the instructional, cultural, research, professional and administrative activities of the District.

An employee may use District computers and the network for union activities in accordance with applicable collective bargaining agreements and policies and procedures governing the use of District equipment. A user is required to behave in a responsible, ethical and legal manner and to follow this procedure and existing Board Policies, Administrative Procedures and local, state and federal laws.

Individual divisions or areas within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Prohibited Uses of District Computer and Network Resources

There are numerous activities and actions that are prohibited while using Computer & Networking resources. These items listed below are some of the main prohibited activities, but it does not represent an all-inclusive exclusive list:

Copyright/License Infringement/Mass Mailings

A user may not participate in any activities knowingly and/or carelessly that have the potential to interfere with or disrupt network users, services, or equipment. The distribution or "forwarding" of spam or unsolicited advertising is strictly prohibited. The District equipment may not be used to violate copyright laws or license agreements. No one may inspect, change, copy or distribute proprietary data, programs, files, disks or software without the proper authority. The prohibited transmission of copyrighted material is forbidden without the express written authorization of the copyright holder.

Computer software protected by copyright must not be copied into, away from, or with the use of campus computing facilities, except as permitted by law or by the terms of the copyright. This means that such computer software may only be copied in order to make back-up copies. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department unless concurrent licensing applies.

Defamation/Libel/Slander

Creating or transmitting any false statement that causes injury to an individual's reputation is strictly prohibited. Any user creating or transmitting defamatory statements shall have sole liability for any damages resulting from such defamatory statement. Any user may also be subject to the District disciplinary procedures for such action.

The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading.

Commercial and Political Use

Commercial use of the District computing systems for personal gain is prohibited. Use for commercial and illegal purposes is unacceptable (e.g. inappropriate mass mailing or "spamming"). This is in direct violation of the Corporation for Education Network Initiatives in California (CENIC) policy under which the District obtains its access to the Internet. (See lines 404-410 of the procedure.) Users also are reminded that the ".cc" and ".edu"

domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

Personal use may be restricted if the resources consumed interfere with equitable access by other users and the utilization of the system for school business purposes.
Direct marketing of personal products and services of any kind is prohibited. Transmitting any unsolicited advertising, promotional materials or other forms of soliciting is prohibited without authorization from District administration.

Links to external sites that market required or recommended instructional materials are allowed only if such links appear in the context of other required and recommended instructional materials, more than one source for such materials is listed, and the materials are available at the campus bookstore and shelved with instructional items.

References on individual web pages to external sites that market non-instructional products and services such as consulting services, etc. are allowed only in the context of a résumé listing.

Links to external sites using direct marketing language such as “consulting services” is not permitted.

The District is a non-profit, tax-exempt organization and, as such, is subject to specific local, state and federal laws regarding sources of income, political activities, use of property and similar matters. District information resources must not be used for partisan political activities that urge the support or defeat of any ballot measure or candidate, or where such use would otherwise be prohibited by local, state, or federal laws, Board Policy or Administrative Procedures.

Use of District Computing System and Resources

Creating, accessing, transmitting, uploading, downloading, printing, or storing sexually explicit, obscene, pornographic, indecent, or lewd material or messages is prohibited, except to the extent that such actions are in furtherance of research or a project that is reasonably and legitimately related to an employee’s position or a student’s coursework.

Processing, transmitting, downloading, or publishing any material in violation of any local, state or federal law is prohibited, including but not limited to the following:

1. Creating, accessing, transmitting, uploading, downloading, printing, or storing sexually explicit, obscene, pornographic, indecent, or lewd material or messages, except to the extent that such actions are in furtherance of research or a project that is reasonably and legitimately related to an employee's position or student's coursework.
2. Creating, accessing, or transmitting material or messages that could be considered discriminatory, offensive, threatening, harassing, intimidating, vulgar, profane, or violent.

3. Creating, accessing, or transmitting material or messages that could be considered defamatory.
4. Violating any state or federal statute or District policy or regulation.
5. Creating, forwarding, or exchanging spam, chain letters, mass postings, solicitations, or advertising.
6. Using District computers, networks, or Internet access for partisan political activities that urge the support or defeat of any ballot measure or candidate, or where such use would otherwise be prohibited by local, state or federal laws, Board Policy or Administrative Procedures.
7. Unauthorized use, duplication, or transmission of copyrighted material or other intellectual property (including software license agreements).
8. Accessing or communicating another individual's password, personal identification number, or other information or files without permission.
9. Using District computers, networks, or Internet access for illegal or unethical activities or unauthorized purposes.
10. Using District computers, networks, or Internet access for personal activities not related to District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.
11. Using District computers, networks, or Internet access for private or personal financial gain, or in connection with non-District consulting, business, or employment.
12. Gaining, attempting to gain, or instructing others as to how to gain unauthorized access to District computers, networks, or Internet access.
13. Obscuring or instructing others as to how to obscure the true identity of a user.
14. Attempting to modify, reconfigure, add, or remove computer equipment, software, hardware, or peripherals without proper authorization.
15. Downloading software onto District computers, hardware, or equipment, or through the District network or Internet connectivity without proper authorization.
16. Vandalizing, damaging, disabling, or destroying District property or the property of another individual or organization.
17. Knowingly engaging in any activity harmful to the District's computers, networks, or Internet access, or to the security or integrity of such systems.
18. Creating, installing, or propagating a computer virus, worm, or other surreptitiously destructive program on any District computer, network, or via District Internet access, regardless of whether any demonstrable harm results.
19. Circumventing or subverting any District computer, network, or Internet security measures or logon procedures.
20. Violating any software license or copyright, including copying, redistributing, storing, or transmitting copyrighted software without the written authorization of the software owner.
21. Sending any fraudulent electronic communication.
22. Willfully interfering with another's authorized computer, network, or Internet usage.
23. Connecting any computer, hardware, or equipment to the District's network, Internet connection, or peripherals without authorization and/or without

confirmation that the computer/hardware/equipment meets the technical and security standards set by the District.

24. Unauthorized distribution of District data and/or proprietary information.
25. Performing any activity that could cause the loss or corruption of, or prevent rightful access to District data or information, or which will interfere with the normal operation of computer, networks, Internet connectivity, or other resources.
26. Creating, accessing, or participating in online gambling.
27. Non-work related or coursework-related uses such as playing games or participating in dating services.
28. Uses in the furtherance of academic dishonesty.
29. Forging, fraudulently altering or falsifying, or otherwise misusing District records or documents.

Viruses and "Hacking"

A user may not upload, transmit, intentionally download, or participate in any manner in the creation, promulgation, publication or use of computer viruses on District resources not designated for such research purposes. A user may not knowingly or carelessly introduce or distribute (i.e. by "forwarding") any invasive or destructive programs (such as viruses, worms, Trojan Horses) in the District computing system.

Engaging in any form of "hacking" (i.e. gaining illegal access) while using the District computing or network systems is prohibited. "Hacking" includes, but is not limited to, gaining access to restricted computer systems/sites and/or viewing, copying, downloading or altering the computer programs, data files, and other materials contained therein.

Improper Use of Private Passwords and Security Devices

A user shall use only his/her/their designated computer account(s) or an appropriate authorized "generic" account to which he/she/they is entitled to access. A user is responsible for his/her/their computer account(s) and shall not allow others to use his/her/their computer account(s). Individual password security is the responsibility of each user. A user may not use any passwords, recognition codes, security access information, or physical locking devices such as locks on any part of the computing system without the District's prior written consent. A user must inform the Director of Information Technology in writing all electronic security devices the user wishes to use prior to using them and provide electronic keys, passwords, access codes and/or other security information or materials to permit the District to obtain access to the user's secured areas. The District reserves the right to remove any such device at any time at the District's discretion.

Users should always maintain their own backups of their protected data as the removal of any private protection systems, of which the District was not aware, could result in unrecoverable data loss. It is a violation for users to protect any assets to which the District has an interest with such systems if the keys are not placed in a proper, authorized escrow with the Director of Information Technology.

System Alterations

Modifying or altering the computing system (except in approved research or for instructional purposes) in any way is prohibited. This includes but is not limited to altering or attempting to alter system software or hardware configurations on either network systems or local computing devices; installing unauthorized software programs on District local computing devices or network systems and/or using such programs; and/or attempting to circumvent local or network system security measures. Modification and alteration of the computing system does not include ordinary operations involving the saving and deleting user generated files that are created in furtherance of District business or educational purposes.

Nondiscrimination/Discriminatory Harassment

A user has the right to be free from any conduct connected with the use of the District's computer and network resources which discriminates against any person on the basis of the categories contained in BP 3410 titled Nondiscrimination. Using the District computer and network resources to transmit any message, create any kind of communication, or store information which violates District policies or procedures regarding discrimination or harassment is prohibited.

Unauthorized Use/Failure to Follow Procedures

Use of the computer and network systems is a privilege extended to students and employees and not a right. An employee user will provide acknowledgement of receipt of the terms and conditions in Administrative Procedure 3720 to the District before the District will provide use privileges. The written acknowledgement will be retained in the employee's personnel file. A student user will be provided notice of the terms and conditions of this Administrative Procedure through the class schedules, the District website and applicable instructional materials.

If substantial amendments, modifications and/or a revocation of the terms and conditions of this Administrative Procedure are made, an employee user will be required to provide a written acknowledgement of receipt of notice of these changes to the Human Resources Office within a reasonable period of time, not to exceed 60 days. Failure to comply with this requirement may result in restriction from computer privileges until the District has received the written acknowledgement. A student user will be notified through the class schedule, the District website and applicable instructional materials.

Each employee or student user is responsible for his/her/their authorized use of the computers and network as described in this Administrative Procedure. Unauthorized use of the computer and/or network system includes:

- Failure to follow the procedures set forth in this procedure and/or
- Engaging in the activities described above, Prohibited Uses of District Computer Resources, of this procedure and/or
- Use of the computer and/or network system in a manner which violates local, state, or federal laws, Board Policy, Administrative Procedures or reasonable rules and regulations of the District or a department and/or

- Use of the computing and/or network system in a manner which damages or harms any person and/or the property of the District and/or
- Any activity or usage of resources that jeopardizes or adds risk to the confidentiality, availability and integrity of District data, computing and network resources.

An employee user who engages in unauthorized or prohibited use of the computer and/or network system may lose computer privileges and/or may be subject to disciplinary action up to and including termination from employment. A student user who engages in unauthorized or prohibited use of the computer and/or network system may lose computer privileges and/or may be subject to disciplinary action up to and including suspension or expulsion.

If allegations of unauthorized or prohibited use are made against a user and the District pursues disciplinary action, disciplinary procedures in this action will follow the applicable Education Code sections and Board Policies.

If a user engages in unauthorized or prohibited use which constitutes a violation of local, state, or federal laws, such violation will be reported to the appropriate law enforcement agency for prosecution as deemed appropriate by the law enforcement or regulatory agency.

Title IV Information Security Compliance

The District shall develop, implement, and maintain a comprehensive information security program that contains all of the following requirements under the Gramm-Leach-Bliley Act.

- A designated employee or employees to coordinate the entity's information security program.
- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the entity's operations, including:
    - Employee training and management;
    - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
- Design and implementation of information safeguards to control the risks the entity identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers, by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

    - By contract, requiring the entity's service providers to implement and maintain such safeguards.
- Evaluate and adjust the entity's information security program in light of the results of the testing and monitoring required; any material changes to the entity's operations or business arrangements; or any other circumstances that the entity knows or has reason to know may have a material impact on the entity's information security program.

Additional Guidelines

The District retains the right to revoke, amend, or change the provisions of this Administrative Procedure for Computer and Network Use. However, any such changes to these procedures will first be reviewed by the Information Technology Standards Committee and the college community shall be informed of such changes through email.

Any defects discovered in computing and network system accounting or system security must be reported promptly to the Director of Information Technology so that steps can be taken to investigate and solve the problem.

Disclosure

A user should be aware that he/she/they does not have an expectation of privacy in the use of District computing and network resources. The District reserves the right to monitor all use of District computer and network system to assure compliance with these procedures. The District will only exercise this right for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the computing system.

A user is advised that there is the possibility of unintended disclosure of communications. A user is advised that it is possible to retrieve information entered on or transmitted via computer and communication systems, even if a user deletes such information.

The California Public Records Act (Government Code, Sections 7920.000 et seq.) includes computer transmissions in the definition of "public records" and communications made on the District network or computing system which is not defined by law as exempt must be disclosed if requested by a member of the public.

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

"CENIC" Policy

CENIC is the District's Internet Service Provider (ISP). District faculty, staff and students are users of the services provided by CENIC and, therefore, must agree to abide by all policies established by CENIC for the use of its network. The latest revision of the CENIC policy is available for viewing at www.cenic.org which may be accessed by using the "Network" tab and selecting "Policies." This CENIC policy is available as a reference for faculty, staff and students to review.

Office of Primary Responsibility: Vice President, Business Services
Vice President, Human Resources

Date Approved: November 26, 2007
Date Revised: May 11, 2015; March 3, 2025
Date Reviewed: January 16, 2019