Origination:	*10/2011*
Last Approved:	*01/2019*
Last Revised:	*01/2017*
Next Review:	*01/2025*
Owner:	*Luke Bixler*
Policy Area:	*Chapter 3 General Institution*
References:	*Legally Advised*

AP 3720 Computer and Network Use

(Replaces current SBCCD AP 3720)

OWNERSHIP RIGHTS

The San Bernardino Community College District ("District") owns, leases, and/or operates a variety of computer and communication systems, including but not limited to: host computers, file servers, work stations, stand-alone computers, laptops, software, and internal or external communications networks (Internet, email, mass notification systems, cloud storage, telephone and voicemail systems). These systems are provided for the use of District faculty, administrators, staff, and students in support of the programs of the colleges and District. Hereinafter, this system and all of its component parts shall be referred to as the "District Network." Modification or Removal of Equipment – Computer users must not attempt to modify or remove computer equipment, software, or peripherals without proper authorization.

PRIVACY INTERESTS

The District recognizes the privacy interests of faculty, staff and students and their rights to freedom of speech, collegial consultation, and academic freedom, as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users anticipate, and may be subject to public disclosure. In addition, the District Network can be subject to authorized and unauthorized access by both internal and external users. For these reasons, there are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the District Network is not to be relied upon as confidential or private.

DISTRICT RIGHTS

System administrators may access users' files or suspend services they manage without notice only: 1) to protect the integrity of computer systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; 4) where evidence exists that violations of law or District Policy or Procedures have occurred. For example, system administrators, following organizational guidelines, may access or examine individual files or accounts based on evidence that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board Policy and/or to protect system integrity.

PASSWORD PROTECTION

A computer user who has be 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.

USAGE

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

MISREPRESENTATION AND LIABILITY

Users of Electronic Communications Resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District unless appropriately authorized to do so. The District is not responsible for any loss or damage incurred by an individual as a result of personal use of the District's Electronic Communications Resources.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Users must not intentionally seek, provide, or release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.

HARRASSMENT

Users are prohibited from using the District's information systems in any way that may be disruptive or offensive to others, including, but not limited to, the intentional viewing and/or transmission of sexually explicit messages, graphics, cartoons, ethnic or racial slurs, or anything that may be construed as harassment or disparagement of others. This is consistent with the District's non-discrimination policy.

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 law or District policy, or which constitute the unauthorized release of confidential information.

COMMERCIAL USE

Commercial use of the District computing resources for personal gain or illegal purposes is prohibited. Computer resources on the District network are provided to support District-related academic and administrative activity. They may not be used for the transmission or storage of commercial, political, or personal advertisements, solicitations and promotions, destructive programs (viruses and/or self-replicating code), or any other unauthorized use. Transmitting unsolicited advertising, promotional materials or other forms of solicitation are prohibited without prior authorization by District administration.

POLITICAL 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.

FAIR USE

Information appearing on the internet should be regarded as copyright protected, whether or not it is expressly noted as such. Section 107 of the Copyright Law (Title 17, US Code) allows for fair use of copyrighted materials. Teaching, scholarship, research, comment, news reporting, and criticism are considered fair and allow for reproduction of a given work. Acknowledgement of the source is recommended but is no substitute for obtaining permission (http://www.copyright.gov/fls/fl102.html).

REPORTING PROBLEMS

Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

SOFTWARE LICENSING

Software, used on District owned computers, must be properly licensed. These licenses provide the acceptable use of the software and hold the user and in some cases the District legally responsible for copyright violations.

All software must be approved by District and/or campus technology departments prior to purchase. Software, its associated license material, and proof of purchase will be submitted and stored with District and/or campus technology departments. For specific District purchasing procedures, please refer to Administrative Procedure 6330.

EXCEPTIONS

Activities will not be considered misuse when authorized by appropriate District officials for security or performance testing. Technology support staff, under the direction of senior management, may at any time examine the equipment, software and services of District owned equipment.

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.

Technology support staff monitors for any unauthorized equipment or software on the District's networks, and reserves the right to remove, disconnect, or disable the unauthorized equipment or software.

NETWORK ACCESS, MEDIA, AND SOCIAL NETWORKING

The District provides network and telecommunications services as a tool for students, staff and faculty. Internet access is provided to assist in the completion of college related work and assignments. As such, the District provides this service and is subject to state and federal regulations. This applies to all equipment attached to the provided network, wired or wireless, without regard to ownership of the equipment. The District recognizes that incidental personal activities may occur provided that such use is within reason, is ordinarily on one's own time, is occasional, and does not interfere with or burden the District's operation. (Please review "Privacy Interests" and "District Rights" sections above.)

Personal social networking accounts shall not be used to officially represent campus or District entities on social networking, wiki, or other social media sites. For official representation of any District entity, a campus or district account, approved by the president/chancellor or their designee, must be used. The account holders must agree to use the resources legally, ethically and in keeping with the intended use per the procedures of their respective sites.

PERSONAL MOBILE DEVICES

The District does not provide support for personal mobile devices. The District only provides the connection settings to the District systems for the synching of District email, calendar and contacts on mobile devices and supported cloud storage files and folders.

The District may also provide the licensing and download methods for software to be used on mobile devices. It is the user's responsibility to install and/or enter settings for such devices and software.

MOBILE DEVICE ENCRYPTION

Any mobile device used by employees to access SBCCD student, employee, financial or other forms of sensitive data will be required to be encrypted prior to such access. This will aide in the protection of District data on lost or stolen mobile devices.

BRING YOUR OWN DEVICE

1. Bring Your Own Device ("BYOD") refers to personally-owned technology devices such as computers, laptops, tablets/eReaders, smart-phones and other devices ("Devices") used by employees for District purposes to stay connected to, access data from, or complete tasks in their capacity as District employees ("Users").

This procedure provides standards and rules of behavior for the use of personal Devices to access District network resources and information for District business purposes. Users may access District information on personal Devices only in the conduct of District business. The District's interests are to foremost protect District data and information while allowing Users to utilize personal Devices.

In accordance with this and other District policies, personal Devices used for business purposes are to be used in a responsible manner. These procedures are mandatory requirements for any Devices used for District purposes.

2. Compliance with District Policies and Administrative Procedures: Users understand that the use of Devices for District purposes is subject to the same District rules and regulations with respect to such use as if the Users are using District-owned devices. Users shall abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of District information. These policies and procedures include, but are not limited to: Computer and Network Use BP/AP 3720; Electronic Mail BP/AP 3920; Student Records Directory Information and Privacy BP/AP 6040; and Records Retention and Destruction BP/AP 3310.

3. Users are Responsible for all Maintenance of their Device(s)

a. Users acknowledge that they are solely responsible for the configuration, maintenance, troubleshooting and repair of their personal Devices. This includes maintaining original device operating systems and keeping the Device current with security patches and updates as released by the manufacturer.

4. Requirements for all BYODs Accessing District network services and District information.

a. Users shall not download, transfer or store “Sensitive Business Data” on their Devices. “Sensitive Business Data” is defined as documents or data that is not publicly available and that is protected by laws governing confidentiality of information (e.g., student records FERPA, confidential personnel data, third party confidential information, etc.). Users shall delete any Sensitive Business Data that may be inadvertently downloaded and stored on the Device (for example, through the process of viewing email attachments sent by others).

The District’s IT Department will provide Users with instructions for identifying and removing these unintended downloads. Users shall not download/transfer Sensitive Business Data to any non-District device.

b. Users shall password protect Devices using existing password protect utilities available on the User’s device. This is inclusive of but not limited to alpha numeric passwords, swipe, finger print and pin codes. Users shall use strong passwords and keep them well protected. It is recommended that when appropriate, Users choose long password of at least 8 characters and change them periodically. Users shall immediately notify the District’s IT Department Help Desk if you believe your passwords have been compromised.

c. Users shall not share the Device with other individuals or family members due to the business use of the Device.

d. Users shall notify the District’s IT Department Help Desk at 877-241-1756 and their cellular providers if the device is lost or stolen within one hour, or as soon as practical, after you notice the device is missing. If the device is a cell phone or tablet with District email the District will remotely wipe the device removing all data from the phone and possible rendering the device unusable in any capacity.

e. If a Device has a remote tracking device, such as the “find my device” option on the iPhone, it should be turned on by the User.

f. Users shall maintain anti-virus (AV) protection on a device when appropriate and possible. Instructions on the recommended AV protection is provided by the District’s IT Department.

g. Users shall set an idle timeout that will automatically lock the Device after a period of time. Users should contact their mobile device manufacturer or service provider for assistance.

5. Compliance with Applicable Laws.

Users must comply with federal and state laws that provide further protections to certain types of information, or that may influence how Users handle District information with the Devices. Examples include, but are not limited to:

a. Family Educational Rights and Privacy Act (FERPA) and corresponding Education Code provisions that provide students right of access to their education records and generally prohibits the disclosure of student education records without the prior written consent of the student.

b. Health Insurance Portability and Accountability Act (HIPAA) which imposes various privacy and security requirements on personal health information collected or maintained by covered entities.

c. Financial Services Modernization Act of 1999 (“Gramm Leach Bliley”) and accompanying FTC Standards for Safeguarding Customer Information Requires the District to develop and implement an information security program designed to protect nonpublic personal information gathered and

maintained with respect to certain financial activities.

d. The Fourth Amendment to the U.S. Constitution, and various federal and state laws concerning access by law enforcement to information and establishes the procedures and circumstances under which law enforcement authorities may gain access to District data. All warrants, subpoenas, and other legal requests, demands, or orders seeking access to institutional data or systems must be forwarded immediately to the District's Human Resources Department.

e. California Public Records Act provides for public access to District records that are not otherwise exempt from disclosure. All requests for records shall be forwarded to the District's Human Resources Department.

f. California invasion of privacy laws that prohibit the disclosure of personal information about an individual.

g. Civil Discovery and E-Discovery Rules, including the duty to preserve data

References:

17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1(b);
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

Attachments

AP 3720 Computer and Network Use - Comments
AP 3720 Computer and Network Use - Legal Citations