Kern Community College District
Board Policy
Chapter 3 – General Institution

BP 3720 COMPUTER AND NETWORK USE

References:

Education Code Section 70902;
Government Code Section 3543.1(b);
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
17 U.S. Code Sections 101 et seq.

NOTE: *The language in red ink is **legally required**.*

Employees and students who use District computers and networks and the information they contain, and related resources have a responsibility not to abuse those resources and to respect the rights of others. The District Chancellor shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

NOTE: *The following language current KCCD Policy 3E is shown as struck because new AP 3720 titled Computer and Network Use addresses many of these issues and similar information. In addition, much of the language in current KCCD Policy 3E is too prescriptive for inclusion in a board policy and might better be reflected in related guidelines, handbooks, manuals, etc.*

*If deemed **critically necessary**, some of the following language could be codified in new **AP** 3720. Another option is to include these prescriptive details on Information Technology webpages and/or in an Information Technology Manual available on the District's website.*

- **From current KCCD Policy 3E titled Information Technology**

~~3E1 **Computing and Network Use**~~

~~3E1A The Kern Community College District shall provide computing and network resources that benefit faculty, staff, and students and support the instructional and~~

~~administrative activities of the Colleges and the District. The District is committed to policies which promote the mission of the Colleges and encourage respect for the rights of individuals. These policies shall apply to all individuals using College and District computing and network resources, regardless of access method.~~

~~3E1B Computing and network resources and all user accounts provided by the Kern Community College District are the property of the Kern Community College District. Access to College/District computing and network resources is a privilege that may be wholly or partially restricted by the Kern Community College District without prior notice and without the consent of the user if required by and consistent with policy or law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs.~~

~~3E1C Employees have no privacy whatsoever in their personal or work-related use of District computers, electronic devices, network and other electronic information resources or to any communications or other information in Kern Community College District computing and network systems or that may be transmitted through Kern Community College District computing and network systems.~~

~~3E1D Kern Community College District retains the right, with or without cause, and with or without notice to the employee, to remotely monitor, physically inspect or examine Kern Community College District computers, electronic devices, network or other computing and network resources and any communication or information stored or transmitted through Kern Community College District computing and network resources including but not limited to software, data, image files, Internet use, emails, text messages and voicemail. Kern Community College District shall exercise this right only when required by and consistent with policy or law, when there is substantiated reason to believe that violations of policy or law have taken place, or in exceptional cases, when required to meet time-dependent, critical operational needs.~~

~~3E1E Use of computing and network resources must be for activities related to the mission of the Colleges and the District. Computing and network resources are to be used in an effective, efficient, ethical, and lawful manner.~~

~~3E1F Use of computing and network resources imposes responsibilities and obligations on the part of users. Users are expected to demonstrate respect for intellectual property, data ownership, system security, individuals' rights to access information, and freedom from intimidation or harassment. (See Procedure 3E1C(a) of this Manual for Computing and Network Use Prohibitions; Policy 3E4 of this Manual for Information Technology Security Policy; Policy 3E3 of this Manual for Email Policy; Procedure 3E1C(b) of this Manual for Computer Software Use Procedures; and Appendix 3E1C of this Manual for the Software Registration form.)~~

~~3E1G Computing and network use shall be consistent with the educational, academic, and administrative purposes of the Colleges/District and shall respect the rights of individuals.~~

~~3E1H The Colleges may develop and implement procedures related to college computing and network use. (See Procedure 3E1F of this Manual for College Computing and Network Use Procedures.)~~

~~3E1I Sanctions for violation of the District/College Computing and Network Use Policies or Procedures may be imposed. Sanctions may range from a warning, to restriction of use, to disciplinary action, and/or legal action.~~

~~3E1J Definition of Kern Community College District Computing and Network Resources includes, but is not limited to:~~

~~Any computer, including a laptop computer, that is:~~

~~Owned, leased, or rented by the Kern Community College District Purchased with funds from a grant awarded to the Kern Community College District~~

~~Borrowed by the Kern Community College District from another agency, company, or entity~~

~~Any electronic device other than a computer that is capable of transmitting, receiving, or storing digital media and is:~~

~~Owned, leased, or rented by the Kern Community College District Purchased with funds from a grant awarded to the Kern Community College District~~

~~Borrowed by the Kern Community College District from another agency, company, or entity~~

~~Electronic devices include, but are not limited to:~~

- ~~Telephones~~
- ~~Cellular Telephones~~
- ~~Push-to-Talk Radios~~
- ~~Pagers~~
- ~~Radios~~
- ~~Digital Cameras~~
- ~~Personal Digital Assistants such as Palm Pilots and Smart Phones~~
- ~~Portable storage devices such as USB thumb drives~~
- ~~Portable media devices such as iPods and MP3 players~~
- ~~Printers and copiers~~
- ~~Fax machines~~

Any component that is used to build or support the Kern Community College District network including, but not limited to:

- Routers
- Switches
- Servers
- Enterprise Storage Systems
- Microwave Components
- Firewalls
- Cabling Infrastructure
- Wireless Access Points and Controllers
- Telephone Switches
- Voicemail Systems
- Network Management and Monitoring Systems

3E2 **Attaching Outside Agencies to the District Wide Area Network (WAN)**

3E2A The Kern Community College District (KCCD) may attach outside agencies to the District Wide Area Network (WAN) when such attachments are mutually beneficial, and consistent with the purposes of the District and its Colleges. These agencies may include, but are not limited to, school districts, hospitals, and police and fire departments.

3E2B The proposal to attach to the District WAN shall be put in the form of a written agreement or contract, and approved by the Board of Trustees or its designee.

3E2C Written proposals will follow the Procedures for implementing these Policies. [See Procedure 3E2E of this Manual for Attaching Outside Agencies to the District-wide Area Network (WAN).]

3E3 **Electronic Mail Policy**

See Procedure 3E3 of this Manual for the Electronic Mail Procedure and Appendix 3E3 for References and Definitions Pertaining to Mail. (Added August 3, 2000)

3E3A The Kern Community College District (KCCD) recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. There is, however, no absolute right to such privacy provided by law; information retained on, or transmitted via, an employer's computer systems is considered the property of the employer.

3E3B KCCD encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's consent. Subject to the requirements for authorization, notification, and other conditions specified in the accompanying Procedure, KCCD may deny access to its electronic mail services and may inspect, monitor, or disclose

electronic mail (a) when required by and consistent with law; (b) when there is substantiated reason to believe that violations of law or of KCCD policies have taken place; (c) when there are compelling circumstances; or (d) under time-dependent, critical operational circumstances.

3E4 **Security Policy** (Added July 9, 2009)

3E4A **Introduction**

Kern Community College District has an obligation to ensure that all Information Technology data, equipment, and processes in its domain of ownership and control are properly secured. This obligation is shared, to varying degrees, by the Colleges and their Centers and every employee of the Kern Community College District. Meeting this obligation is critical to achieving Kern Community College District's mission of providing outstanding educational programs and services that are responsive to our diverse students and communities.

In order to carry out its mission, Kern Community College District shall provide secure yet open and accessible Information Technology resources to all employees and students. Toward this end, Kern Community College District will strive to balance its Information Technology Security Program efforts with identified risks that threaten the availability and performance of mission critical computing and network resources.

Kern Community College District shall ensure that the use of Information Technology resources complies with the appropriate Kern Community College District policies and procedures and applicable Federal and State regulations.

3E4A1 Definitions

a. Information Technology Resources: people, processes, and technology needed to deliver Information Technology services (Banner, e-mail, online classes, etc.) to Kern Community College District employees and students.

b. Computing and Network Resources: any and all technology (servers, personal computers, applications, laptops, routers, etc.) that make up Kern Community College District's vast Information Technology operation.

3E4B **Scope of Information Technology Security**

3E4B1 Information Technology Security Defined

Information Technology Security is defined as the state of being relatively free of risk. This risk concerns the following categories of losses:

a. Confidentiality of Information Technology data or privacy of personal data and college data

b. Integrity or accuracy of personal data and college data stored in Information Technology systems

c. Information Technology assets which include Information Technology systems, networks, facilities, programs, documentation, and data

d. Personal and college data stored in Information Technology systems Information Technology Security is also viewed as balancing the implementation of security measures against the risks that have been identified and weighted against the effective operation of the Kern Community College District.

3E4B2 **Domains of Information Technology Security**

Kern Community College District's Information Technology Security shall deal with the following domains of security:

a. Computer Systems' Security: servers, workstations, applications, laptops, mobile devices, operating systems, and related peripherals used by Kern Community College District employees and students

b. Network and Communications Security: all equipment, people, and processes in place to operate Kern Community College District's network and communications infrastructure

c. Physical Security: premises occupied by Information Technology personnel and core (not end-user) Information Technology equipment such as servers, routers, and switches

d. Operational Security: environmental systems such as HVAC, power, and other related operational systems

3E4B3 **Information Technology Security Program**

Kern Community College District shall have an Information Technology Security Program comprised of the following components:

a. A framework for classifying, reviewing, and updating Kern Community College District's Security risk posture (Risk Assessment)

A framework for identifying location, type, sensitivity, and access requirements for all data residing anywhere within the Kern Community College District

Documentation of Information Technology Security Program roles, responsibilities, processes, and architecture

A plan for identifying, prioritizing, and addressing applicable Federal, State, and other legal compliance requirements

Appropriate Information Technology Security policies, procedures, and guidelines

An Information Technology Security Awareness and Information Dissemination plan

A plan for identifying, validating, prioritizing, implementing, and auditing Information Technology security technology initiatives needed to effectively secure Kern Community College District's Information Technology operations

3E4C **Roles and Responsibilities**

3E4C1 Within the context of Information Technology Security, all Kern Community College District employees and students are responsible to some degree for safeguarding the Information Technology resources they use. Equally, all Kern Community College District employees and students are expected to comply with all Kern Community College District Information Technology Security policies and related procedures.

3E4C2 The Information Technology Managers from the three Colleges and the District Office are responsible for Information Technology Security throughout Kern Community College District.

3E4C3 Kern Community College District's Director, Information Technology is responsible for carrying out Kern Community College District's Information Technology Security Program as outlined in Policy 3E4B3 .

3E4C4 Appropriate College and District-wide committees shall have the opportunity to provide input on the development of Information Technology Security policies and procedures.

3E4D **Sanctions**

3E4D1 Violations of this policy are subject to the established Kern Community College District disciplinary processes as outlined in Kern Community College District Board Policy and Kern Community College District employee contracts.

Acknowledgements: Kern Community College District acknowledges Murdoch University of Perth, Western Australia (www.murdoch.edu.au), and the University of Minnesota (www.umn.edu) for allowing Kern Community College District to use their Information Technology Security policy material.

Kern Community College District
Administrative Procedure
Chapter 3 – General Institution

AP 3720 COMPUTER AND NETWORK USE

References:

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

NOTE: *The following language in red ink is **legally advised**. Local practice may be inserted. The following is an illustrative example:*

The District Computer and Network systems are the sole property of the District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, ~~mainframes, minicomputers~~, servers, network equipment, storage devices, and associated peripherals, software, and information resources, regardless of whether used for administration, research, teaching, or other purposes.

Conditions of Use

Individual units 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, or restrictions.

Legal Process

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to

loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action.

Copyrights and Licenses
Computer users must respect copyrights and licenses to software and other on-line 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 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.*
>
> ***Number of Simultaneous Users*** *- The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.*
>
> ***Copyrights*** *- In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.*

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

NOTE: Districts may reference the electronic information security standard created by the California Community Colleges Technology Center.

> ***Modification or Removal of Equipment*** *- Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.*
>
> ***Unauthorized Use*** *- Computer users must not interfere with other's access and use of the District's computers, data, network, or other electronic and information resources. This includes but is not limited to:*
>
> - *using or consuming excessive resources without a legitimate academic or business purpose (e.g. sending bulk email or downloading large amounts of data for personal use)*
> - *printing excessive copies of documents or personal material*
> - *bypassing or attempting to bypass a computer or network security measure*
> - *causing or attempting to cause a "denial of service" condition on any network or system*
> - *unauthorized modification of data*
> - *unauthorized modification of a district computer system*

- *unauthorized access to district data or the data of another user*
- *unauthorized disclosure of personally identifiable information or other information protected by state or federal law*
- *sharing a district account or password with another user without proper authorization*
- *using a district account or password assigned to another user without proper authorization*
- *physically damaging or vandalizing any district computer system or equipment.*
- ~~*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 system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, 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 the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings. Unauthorized programs include but are not limited to: viruses, Trojan horses, worms, ransomware, keyloggers, exploits, backdoors and rootkits.*

Academic Purposes – Faculty may explore computer security issues, including methods for bypassing protection measures, for the purpose of academic research, and students may do so as a part of an approved academic course or program, provided that such activity is confined to an environment that is designated for such use and the activity does not negatively impact the security of the district and does not negatively impact other users or district resources.

Security Testing – The district may authorize system administrators or contracted third parties to conduct security assessments and tests of the district's computer and network resources.

Unauthorized Access

Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Abuse of Computing Privileges *- Users of District information resources must not access computers, computer software, computer data, or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in*

question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

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.*

Password Protection *- A computer user who has been 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.~~ District.*

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.

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 Usage *- Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). ~~Some public discussion groups have been designated for selling items by [**insert names of groups, if any**] and may be used appropriately, according to the stated purpose of the group(s).~~*

Information Belonging to Others *- Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.*

Rights of Individuals *- Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.*

User Identification *– Users shall not send email or other electronic messages with spoofed or misleading account names or identification.*

~~***User identification*** *- Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.~~

Political, Personal, 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.*

Political Use *- District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.*

Personal Use *- District information resources should not be used for personal activities not related to District functions, except in a purely incidental or minimal 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.*

Obscene Material *– District computer and network resources may not be used to intentionally transmit, receive, display or copy obscene or pornographic material.*

Commercial Use *- District information resources should not be used for commercial purposes. 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.*

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the District network and computer resources which discriminates against any person on the basis of the protected categories cited in BP 3410 titled Nondiscrimination. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

No Expectation of Privacy *- The District reserves the right to monitor all use of the District network and computer systems to assure compliance with these policies and to ensure the operation, performance and security of these systems. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes~~, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.~~*

Possibility of Disclosure *- Users must be aware of the possibility of unintended disclosure of communications.*

Retrieval *- It is possible for information entered on, stored, 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 network or computers must be disclosed if requested by a member of the public.

***Litigation and Public Records** - Computer transmissions and electronically stored information may be discoverable in litigation or subject to a public records request.*

Dissemination and User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

~~A "pop-up" screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The "pop-up" screen shall appear prior to accessing the e-mail network.~~ To the extent that it is technically feasible, a warning banner will be displayed on all district computer systems summarizing and acknowledging this policy, and warning users that they have no expectation of privacy. Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:

***Computer and Network Use Agreement** (Sample Language)*

I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the procedures for the duration of my employment or enrollment. I am aware that violations of this Computer and Network Use Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of state or federal law.

NOTE: *The following language current KCCD Procedure 3E1C(a) is shown as struck because new AP 3720 titled Computer and Network Use addresses many of these issues and similar information (above).*

*If deemed **critically necessary**, some of the following language could be codified in this new **AP 3720** (above). Another option is to include these prescriptive details on Information Technology webpages and/or in an Information Technology Manual available on the District's website.*

- **From current KCCD Procedure 3E1C(a) titled Computing and Network Use Prohibitions**

~~Improper uses of Colleges/District computing and network resources are prohibited as follows:~~

~~(1) The use of computing and network resources for cheating, plagiarism, furnishing false information, other acts of academic dishonesty, or malicious behavior that interferes with meeting the College/District educational mission is prohibited.~~

~~(2) The use of computing and network resources shall not interfere with the work of employees or students nor disrupt the normal operation of the Colleges/District.~~

~~(3) Computing and network use that monopolizes resources; network use that creates unnecessary network traffic; broadcast of inappropriate electronic mail and messages; transmission of electronic chain letters or other requests for money; and distribution or circulation of media known or suspected to contain computer viruses are prohibited.~~

~~(4) Copying, distributing (either free or for monetary gain), or receiving copyrighted software or electronic information without paying the specified royalty (U.S. copyright laws) are prohibited.~~

~~(5) Unauthorized computing and network account sharing is prohibited.~~

~~(6) Attempts to gain unauthorized access to any computing or network resource are prohibited.~~

~~(7) Unauthorized commercial or business use of Colleges/District computing and network resources for individual or private gain is prohibited.~~

~~(8) Use of Colleges/District computing and network resources to intentionally transmit, receive, display or copy obscene, pornographic, discriminatory or harassing materials not related to coursework or research is prohibited.~~

~~(9) Use of Colleges/District computing and network resources to access or attempt to access student or employee information for any purpose not specifically job-related violates state and federal laws and District policy and is prohibited.~~

~~(10) The Electronic Communications Privacy Act (federal law) includes electronic mail and messages in the same category as U.S. mail and telephone calls, and defines unauthorized attempts to access another user's information as unlawful behavior. Such behavior is prohibited.~~

~~Reviewed and Recommended by~~
~~Chancellor's Cabinet, September 16, 2008~~
~~District Consultation Council, May 18, 2009~~

NOTE: *The following language current KCCD Procedure 3E1C(b) is shown as struck because new AP 3720 titled Computer and Network Use addresses many of these issues and similar information (above).*

*If deemed **critically necessary**, some of the following language could be codified in this new **AP 3720** (above). Another option is to include these prescriptive details on Information Technology webpages and/or in an Information Technology Manual available on the District's website.*

- **From current KCCD Procedure 3E1C(b) titled Computer Software Use Procedures**

~~(1) Only software which falls into one of the following categories may be used on equipment which is under the jurisdiction of the Kern Community College District:~~

~~a) The software has been purchased by the District in sufficient quantities to account for one purchase for each machine on which the software is used, and a written record of the purchase is available in District files.~~

~~b) The software is covered by a licensing agreement with the software author, vendor, or developer, as applicable; no tenets of the agreement have been violated by the user; and a written copy of the agreement is available in District files.~~

~~c) The software has been donated to the District in accordance with the software license, and a written record of the donation or its acceptance is available in District files.~~

~~d) The software has been developed or written by a District employee for use on District equipment, and full credit has been given to the developer by other users.~~

~~e) The software is in the public domain, and documentation exists to substantiate its public domain status.~~

~~f) The software is being reviewed or demonstrated as part of a purchasing or licensing decision, and arrangements for such review or demonstration have been satisfactorily reached between the District and the appropriate vendor or representative.~~

~~g) The software is the personal property of the user, and these procedures and software license requirements are followed.~~

~~(2) According to law, all copies are illegal unless they fall into one of the following categories:~~

~~a) The copy is created as an essential step in the utilization of the computer program in conjunction with a machine, and it is used in no other manner.~~

~~b) The copy is for archival purposes only, and all archival copies are destroyed when continued possession of the computer program ceases to be rightful.~~

c) The copy is in compliance with the license agreement.

(3) In order to certify the District's right-to-use software installed on District-owned computers, copies of all software licenses shall be on file at a designated location. When installing software on a District-owned computer, the person completing the installation is responsible for the following:

a) Installation of the software according to instructions provided by the software author/distributor.

b) Completion of a Software Registration Form. (See Appendix 3E3)

c) Forwarding the Software Registration Form, the Software License Agreement received with the software, and a copy of the software purchase order to the designated location. These documents constitute an archival record.

(4) If a software audit is performed either by District staff, law enforcement officers, or regulatory agencies, the archival records will be used to prove ownership of specific software products. If an archival record does not exist for a specific copy of software and the user is unable to provide proof of legal use as stated in these Procedures, the software will be deleted from the computer's storage media, and all backup copies will be destroyed.

Approved by the Chancellor's Cabinet
May 23, 1993
Renumbered 4/21/94, 2/11/97, and 10/11/00

Also see BP/AP 3710 titled Securing of Copyright and AP 3750 titled Use of Copyrighted Material

NOTE: *The following language current KCCD Procedure 3E1F is shown as struck because new AP 3720 titled Computer and Network Use addresses some of these issues and similar information (above).*

*If deemed **critically necessary**, some of the following language could be codified in this new **AP 3720** (above). Another option is to include these prescriptive details on Information Technology webpages and/or in an Information Technology Manual available on the District's website.*

- **From current KCCD Procedure 3E1F titled College Computing and Network Use Procedures**

The Colleges of the Kern Community College District may develop, adopt, and implement written computing and network use procedures that are consistent with the District's Computing and Network Use Policy, including, but not limited to references to:

A. The District Computing and Network Use Policy including its ten (10) prohibitions.

B. The legal aspects of computing and network use procedures such as:

1) The rights of users to freely examine issues.

2) Sexual harassment and creating a hostile environment

3) Freedom from intimidation, embarrassment, or fear

4) Rules related to behavior

C. The development of priorities that emphasize computing and network use that is related to the mission of the College/District.

D. Sanctions that range from a warning, to restriction of use, to disciplinary action, to legal action.

E. College Computing and Network Use Procedures will have the approval of the President, will be given wide dissemination to users, and will be forwarded to the District Director, Information Technology.

Reviewed and Recommended by
Chancellor's Cabinet
September 16, 2008

Reviewed and Recommended by
District Consultation Council
May 18, 2009

NOTE: *The following language current KCCD Procedure 3E2E is shown as struck as it is unique to the District, and these details are recommended for inclusion on Information Technology webpages and/or in an Information Technology Manual available on the District's website (or on the District's intranet system).*

- **From current KCCD Procedure 3E2E titled Attaching Outside Agencies to the District Wide Area Network (WAN)**

1. A written proposal to attach outside agencies to the District WAN is required, and must meet the following stipulations:

a) Cite and explain the mutual benefit to the District and the outside agency of the proposed attachment.

b) Identify the costs required to establish and maintain the proposed attachment with the assistance of the District Information Technology staff. Cost considerations should include, but not be limited to, the following:

- Hardware costs
- Support costs
- Bandwidth costs
- Personnel costs
- Other costs

c) Propose the method for either recovering the related costs, and/or demonstrating the quantifiable off-setting financial benefits to the KCCD.

d) Specify the proposed terms and conditions, which include the following:

- Duration of the agreement and means for evaluating whether it should be extended, renewed, or terminated
- Services to be provided
- Costs to the District and method of cost recovery and/or reimbursement
- Disclaimers related to the interruptions outside the control of KCCD
- Mutually agreed upon security provisions
- Method of distribution of resources and obligations upon dissolution of agreement

2. A proposal following the stipulations set forth in the Procedures noted in #1, above, will be presented to the District-wide Information Technology Committee (DWITC) for consideration, with action following at a subsequent meeting.

3. The DWITC recommendation will be taken to the Chancellor's Cabinet for consideration.

4. The agreement or contract for attaching the outside agency to the District WAN will be taken to the Board of Trustees for action upon the recommendation of the Chancellor's Cabinet.

5. Once the proposal to attach an outside agency to the District WAN is approved, the Assistant Chancellor, Information Technology will implement the agreement and proceed with the project.

Approved by the Chancellor's Cabinet
February 8, 2000

NOTE: *The following language current KCCD Procedure 3E3 is shown as struck. If deemed **critically necessary**, some of the following language could be codified in this new **AP 3720** (above). Another option is to include these prescriptive details on Information Technology webpages and/or in an Information Technology Manual available on the District's website.*

- **From current KCCD Procedure 3E3 titled Electronic Mail Procedure**

PART ONE—INTRODUCTION

The purpose of this Procedure is to assure that:

1. The Kern Community College District (KCCD) community is informed about the applicability of policies and laws to electronic mail;

2. Electronic mail services are used in compliance with those policies and laws;

3. E-mail users are informed about how concepts of privacy and security apply to electronic mail; and

4. Disruptions to KCCD electronic mail and other services and activities are minimized.

PART TWO—DEFINITIONS

Any readers unfamiliar with the terminology used in this Procedure can refer to a set of definitions in Appendix 3E3, Part C.

PART THREE--GENERAL INFORMATION

General information regarding electronic mail has been included in Appendix 3E3, Part D.

PART FOUR—SCOPE

This Procedure applies to:

1. All electronic mail systems and services provided or owned by the KCCD.

2. All users, holders, and uses of KCCD E-mail services.

3. All KCCD E-mail records in the possession of KCCD employees or other E-mail users of electronic mail services provided by the KCCD.

This Procedure applies only to electronic mail in its electronic form. The Procedure does not apply to printed copies of electronic mail.

PART FIVE--GENERAL PROVISIONS

1. **Purpose--**In support of its mission of instruction and public service, the KCCD encourages the use of KCCD electronic mail services to share information, to improve communication, and to exchange ideas.

2. **KCCD Property--**KCCD electronic mail systems and services are KCCD facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with KCCD, or any sub-unit of the KCCD, assigned by the KCCD to individuals, sub-units, or functions of the KCCD, is the property of the KCCD.

3. **Service Restrictions--**Those who use KCCD electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of KCCD, and with normal standards of professional and personal courtesy and conduct. Access to KCCD electronic mail services is a privilege that may be wholly or partially restricted by KCCD without prior notice and without the consent of the E-mail user when required by and consistent with law, when there is substantiated reason (as defined in Appendix 3E3, Part C, Definitions) to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs.

4. **Consent and Compliance--**An E-mail holder's consent shall be sought by KCCD prior to any inspection, monitoring, or disclosure of KCCD E-mail records in the holder's possession, except as provided for in Part Five, Number 5. KCCD employees are, however, expected to comply with KCCD requests for copies of E-mail records in their possession that pertain to the administrative business of KCCD, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by KCCD. Failure to comply with such requests can lead to the conditions of Part Five, Number 5.

5. **Restrictions on Access Without Consent--**KCCD shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such E-mail (a) when required by and consistent with law; (b) when there is substantiated reason (as defined in Appendix 3E3, Part C, Definitions) to believe that violations of law or KCCD policies listed in Appendix 3E3, Part B have taken

place; (c) when there are compelling circumstances as defined in Part Three; or (d) under time-dependent, critical operational circumstances as defined in Appendix 3E3, Part C, Definitions.

When the contents of E-mail must be inspected, monitored, or disclosed without the holder's consent, the following shall apply:

(A) Authorization--Except in emergency circumstances as defined in Appendix 3E3, Part C, Definitions, and pursuant to Part Five, Number 5b, such actions must be authorized in advance and in writing by KCCD Assistant Chancellor for Information Technology Services (IT). Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

(B) Emergency Circumstances--In emergency circumstances as defined in Appendix 3E3, Part C, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Part Five, Number 5A, above.

(C) Notification--In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other KCCD policies and procedures, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

(D) Compliance with Law--Actions taken under Part Five, Numbers 1 and 2 shall be in full compliance with the law and other applicable KCCD policy and procedure, including laws and policies listed in Appendix 3E3, Part A.

6. **Recourse**--Individuals who believe that actions taken by employees or agents of KCCD were in violation of this Procedure should file a complaint with the Assistant Chancellor for IT.

7. **Misuse**--In general, both law and KCCD policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies (see Appendix 3E3, Part A, References).

PART SIX--SPECIFIC PROVISIONS

1. Allowable Use--In general, use of KCCD electronic mail services is governed by policies that apply to the use of all KCCD facilities. In particular, use of KCCD electronic mail services is encouraged and is allowable subject to the following conditions:

(A) **Purpose**--Electronic mail services are to be provided by KCCD organizational units in support of the teaching, research, and public service mission of KCCD, and the administrative functions that support this mission.

(B) **Users**--Users of KCCD electronic mail services are to be limited primarily to KCCD students, faculty, staff, and community users for purposes that conform to the requirements of this Section.

(C) **Non-Competition--**KCCD electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the KCCD.

(D) **Restrictions**--KCCD electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of KCCD; personal financial gain (see applicable academic personnel policies); personal use inconsistent with Part Six, Number 1H; or uses that violate other KCCD policies or guidelines. The latter include, but are not limited to, policies and guidelines (see Appendix 3E3, Part A, References) regarding intellectual property, or regarding sexual or other forms of harassment.

(E) **Representation**--Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of KCCD or any unit of KCCD unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing KCCD. (e.g., "These opinions are my own, not those of KCCD.")

(F) **False Identity--**KCCD E-mail users shall not employ a false identity. E-mail may, however, be sent anonymously, provided this does not violate any law or any KCCD policy, and does not unreasonably interfere with the administrative business of KCCD.

(G) **Interference--**KCCD E-mail services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of E-mail or E-mail systems. Such uses include, but are not limited to, the use of E-mail services to: (a) send or forward Email chain letters; (b) "spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited E-mail; and (c) "letter-bomb," that is, to resend the same E-mail repeatedly to one or more recipients to interfere with the recipient's use of E-mail.

(H) **Personal Use**--KCCD electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the KCCD operation of computing facilities or electronic mail services; (ii) burden the KCCD with noticeable incremental cost; or (iii) interfere with the E-mail user's employment or other obligations to the KCCD.

2. **Security and Confidentiality**

(A) The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Procedure, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using E-mail to communicate confidential or sensitive matters.

(B) Users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of KCCD E-mail services, and on these and other occasions may inadvertently see the contents of E-mail messages. Except as provided elsewhere in this Procedure, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect E-mail when re-routing or disposing of otherwise undeliverable E-mail. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable E-mail to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the E-mail has been inspected for such purposes.

(C) The KCCD attempts to provide secure and reliable E-mail services. Operators of KCCD electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of E-mail services have no control over the security of E-mail that has been downloaded to a user's computer. As a deterrent to potential intruders and to misuse of E-mail, E-mail users should employ whatever protections (such as passwords) are available to them.

(D) Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may

be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process copies data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail.

3. **Archiving and Retention**

(A) KCCD does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up only to assure system integrity and reliability, not to provide for future retrieval. Operators of KCCD electronic mail services are not required by this Procedure to retrieve E-mail from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

(B) E-mail users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Part One, Number 4), it is difficult to guarantee that E-mail documents have not been altered, intentionally or inadvertently.

(C) E-mail users and those in possession of KCCD records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acidfree paper or microfilm, where long-term accessibility is an issue.

PART SEVEN--PROCEDURE VIOLATIONS

Violations of KCCD procedures governing the use of KCCD electronic mail services may result in restriction of access to KCCD information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other KCCD policies, guidelines, implementing procedures, or collective bargaining agreements.

PART EIGHT--RESPONSIBILITY FOR PROCEDURE

The Assistant Chancellor for IT is responsible for development and maintenance of this Procedure, with the concurrence of the District-Wide IT Committee (DWITC).

Approved by Chancellor's Cabinet

~~March 28, 2000~~