Kern Community College District
Administrative Procedures
Chapter 3 – General Institution

AP 3720 COMPUTING 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: This procedure is **legally advised.**

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, servers, network equipment, storage devices and associated peripherals, software and information resources, cloud and on-premises solutions, 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.

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 attempt to access confidential information without a legitimate district business purpose and 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
- Accessing or attempting to access confidential student or employee information for any purpose not specifically job-related or otherwise authorized by the district.
- 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.

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 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).

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 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 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 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 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.

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. Logging into our systems will acknowledge

compliance with policies. At initial employment 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 Usage 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.

Title IV Information Security Compliance

- 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:

(1) Employee training and management;

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

(3) 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:

  (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

  (2) Requiring the entity's service providers by contract 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.

- The District and its colleges adopt as their security standard they will adhere to National Institutes of Standards and Technology Special Publication 800-171 ("NIST SP800-171"). This document outlines requirements for protected "Controlled Unclassified Information (CUI)" and is recommended as a model and standard by the United States Department of Education in order to meet the requirements of the Student Aid Information Gateway (SAIG) Enrollment Agreement and the Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA).

- **Information Security Responsibilities**

- The college and district IT managers are responsible for Information Technology Security within their assigned areas. The district Director of IT Security maintains overall responsibility for IT security throughout the district, is responsible for carrying out the district's Information Technology Security program and is responsible for overseeing district-wide IT security operations.

- Additionally, all District employees, students, and other users of district technology resources, bear some degree of responsibility for safeguarding the technology resources they use. Accordingly, all users of the district's technology resources are expected to comply with the district's Information Technology Security policies and related procedures.

Prohibitions of Use

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. *S*uch behavior is prohibited.

Software Use

(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.

(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.

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:

1. The District Computing and Network Use Policy including its ten (10) prohibitions.
2. 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

3. The development of priorities that emphasize computing and network use that is related to the mission of the College/District.
4. Sanctions that range from a warning to restriction of use, to disciplinary action, to legal action.
5. 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.

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.

Electronic Mail Procedure

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.

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.

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 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 to believe that violations of law or KCCD policies;

   (c) when there are compelling circumstances as defined in Part Three; or

   (d) under time-dependent, critical operational circumstances.

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

1. (A) Authorization--Except in emergency circumstances 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.
2. (B) Emergency Circumstances--In emergency circumstances 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.
3. (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.

6. (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.
7. **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.
8. **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

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 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 E-mail 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. KCCD email is subject to a 2-year retention cycle.

(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.

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.

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