

# Computer Use and Electronic Mail Guidelines

## Antelope Valley College District

Office of the President

Developed 04/23/01

Current revision 03/22/06

### Table of Contents

Part One: Computer Resources .....	2
1. Introduction .....	2
2. Definitions.....	2
3. Rights and Responsibilities .....	4
4. General Provisions .....	5
5. Existing Legal Context.....	6
6. Appropriate Use.....	7
7. Examples of Inappropriate Use.....	7
8. Enforcement .....	8
9. Procedure for Review.....	9
Part Two: E-mail Use Highlights .....	10
Part Three: Complete Electronic Mail Guidelines.....	12
10. Introduction.....	12
11. Purpose .....	13
12. Scope .....	13
13. Specific Provisions.....	14
14. Policy Violations.....	17
15. Responsibility for Guidelines.....	17
16. College Responsibilities and Discretions.....	17
Appendix A: Privacy and Public Records Issues.....	19

## Part One: Computer Resources

### 1. Introduction

- 1.1 In support of Antelope Valley College (AVC)'s educational mission, Information Technology Services (ITS) provides computing facilities, networking and information technology resources for the use of students, employees and board members.
- 1.2 These Computer Use and Electronic Mail Guidelines govern the use of computer equipment, services and networks on the campus. As a user of these resources, you are responsible for reading and understanding this document.
- 1.3 Internet access is provided to the campus via the Corporation for Education and Network Initiatives in California (CENIC). CENIC's California Research and Education Network – Digital California (CalREN-DC) provides high-quality network services for K-20 students and employees. As a CENIC Associate, Antelope Valley College must ensure that the AVC user community complies with the CalREN Acceptable Use Policy (AUP). In order to ensure compliance, the AVC Computer Use and Electronic Mail Guidelines (this document) incorporate the same terms specified by the CalREN AUP.
- 1.4 The college recognizes that principles of academic freedom and participatory governance, freedom of speech and privacy of information hold important implications for computer use, particularly the use of electronic mail and electronic mail services. The college affords computer file and electronic mail privacy protections comparable to that which it traditionally affords paper documents and telephone communications. These guidelines reflect these firmly held principles within the context of the college's legal and other obligations.

### 2. Definitions

**College E-mail Record:** A college record in the form of an e-mail record regardless of whether any of the computing facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read or print the e-mail record is owned by the college. This implies that the location of the record or the location of its creation or use, does not change its nature as: (i) a college e-mail record for purposes of this or other college policy and (ii) having potential for disclosure under the California Public Records Act.

Until determined otherwise or unless it is clear from the context, any e-mail record residing on college-owned computing facilities may be deemed to be a college e-mail record for purposes of these guidelines. Consistent, however, with the principles asserted in Section 4.5 of least perusal and least action necessary and of legal compliance, the college must make a good faith a priori effort to distinguish college e-mail records from personal and other e-mail where relevant to disclosures under the California Public Records Act and other laws or for other applicable purposes of these guidelines.

**College E-mail Systems or Services:** Electronic mail systems or services owned or operated by the college or any of its sub-units. College electronic mail systems and services are college facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with the college, assigned by the college to individuals or to functions of the college, is the property of the Antelope Valley College District.

**College Record:** A "public record" as defined in the California Public Records Act. "Public records" include any writing containing information relating to the conduct of the public's business prepared, owned, used or retained (by the college) regardless of physical form or characteristics. [California Government Code Section 6252(e)]. With certain defined exceptions, such college records are subject to disclosure under the California Public Records Act.

Records held by students, including e-mail, are not college records unless such records are pursuant to an employment or agent relationship the student has or has had with the college. This exemption does not, however, exclude student e-mail from other aspects of these guidelines, regardless of whether such e-mail is a college record.

**Compelling Circumstances:** Circumstances where time is of the essence and failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of college policies or significant liability to the college or to members of the college community.

**Computing Facility(ies):** Computing resources, services (including e-mail) and network systems, such as computers and computer time, data processing or storage functions, computer systems and services, servers, networks, input/output and connecting devices and related computer records, programs, software and documentation.

**E-mail Record or E-mail:** Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read or printed by one or several e-mail systems or services. This definition of e-mail records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses and addressees. These guidelines apply only to electronic mail in its electronic form. The guidelines do not apply to printed copies of electronic mail.

**Electronic Mail Systems or Services:** Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail or is implicitly used for such purposes, including services such as electronic bulletin boards, listservers and newsgroups.

**Holder of an E-mail Record or E-mail Holder:** An e-mail user who is in possession of a particular e-mail record, regardless of whether that e-mail user is the original creator or a recipient of the content of the record.

**Possession of E-mail:** An individual is in "possession" of an e-mail record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage. Thus, an e-mail record that resides on a computer server awaiting download to an addressee is deemed, for purposes of these guidelines, to be in the possession of that addressee. Systems administrators and other operators of college e-mail services are excluded from this definition of possession with regard to e-mail not specifically created by or addressed to them.

E-mail users are not responsible for e-mail in their possession when they have no knowledge of its existence or contents.

**Substantiated Reason:** Reliable evidence indicating that violation of law or of college policies probably has occurred, as distinguished from rumor, gossip or other unreliable evidence.

**Time-dependent and Critical Operational Circumstances:** Circumstances where failure to act could seriously hamper the ability of the college to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities or to faculty research or matters of participatory governance.

**Use of College or Other E-mail Services:** To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read or print e-mail (with the aid of college e-mail services). A (college) e-mail user is an individual who makes use of (college) e-mail services.

Receipt of e-mail prior to actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the e-mail record.

**User:** Any individual or group who uses college computing facilities.

### **3. Rights and Responsibilities**

3.1 Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources and observe all relevant laws, regulations and contractual obligations.

3.2 Faculty and staff, as well as students, may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines (see Section 4.5), system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse or that have been corrupted or damaged.

#### 4. General Provisions

- 4.1 Purpose. In support of its educational mission, the college encourages the use of its computing facilities to manage and share information, to improve communication and to develop and exchange ideas.
- 4.2 Service Restrictions. Those who use college computing facilities are expected to do so responsibly, that is, to comply with state and federal laws, with these guidelines and policies and procedures of the college and with normal standards of professional and personal courtesy and conduct. Access to college computing facilities may be wholly or partially restricted by the college without prior notice and without the consent of the user when 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. Such restriction is subject to established district procedures or, in the absence of such procedures, to the approval of the college president or appropriate vice president.
- 4.3 Consent and Compliance. A user's consent shall be obtained by the college prior to any inspection, monitoring or disclosure of college computer files or e-mail records in the holder's possession, except as provided for in Section 4.4. College employees are, however, expected to comply with college requests for copies of computer files or e-mail records in their possession that pertain to the administrative business of the college or whose disclosure is required to comply with applicable laws.
- 4.4 Restrictions on Access Without Consent. The college shall permit the inspection, monitoring or disclosure of computer files or electronic mail without the consent of the user (i) when consistent with law; (ii) when there is substantiated reason to believe that violations of law or of college policies have taken place; (iii) when there are compelling circumstances; or (iv) under time-dependent, critical operational circumstances.
- 4.5 When the contents of computer files or e-mail must be inspected, monitored or disclosed without the user's consent, the following shall apply:
- 4.5.1 Authorization. Except in compelling circumstances, such actions must be authorized in advance and signed by the college president or responsible vice president. This authority may not be further re-delegated. Requests for such non-consensual access must be submitted in writing to the college president or responsible vice president. College counsel's advice shall be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of computer files and electronic mail and because of potential conflicts among different applicable laws.
  - 4.5.2 Compelling Circumstances. In compelling circumstances, the least perusal of contents and the least action necessary to resolve the situation may be taken immediately without authorization, but appropriate authorization

must then be obtained without delay following the procedures described in Section 4.5.1.

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

4.5.4 Compliance with Law. Actions taken under Sections 4.5.1 and 4.5.2 shall be in full compliance with the law and applicable college policy.

4.6 Recourse. The review and appeal of actions taken under Section 4.2, 4.3, 4.4 or 4.5 may be requested by individuals who believe that actions taken by employees or agents of the college were in violation of these guidelines. Requests for review and appeal may be submitted to the individual's supervisor or to the Human Resources department for investigation.

4.7 Misuse. In general, both law and college policies prohibit the theft or other abuse of computing facilities. Such prohibitions also 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 college computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of college computing facilities are encouraged to familiarize themselves with these laws and college policies.

## **5. Existing Legal Context**

5.1 All existing laws (federal and state) and AVC regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

5.2 Users do not own accounts on AVC computers, but accounts are assigned to individuals for use in conducting college business. Under the [Electronic Communications Privacy Act of 1986](#) users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other AVC employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the college. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, student files on college computer facilities are considered "educational records" under the [Family Educational Rights and Privacy Act of 1974](#).

5.3 Misuse of computing, networking or information technology resources may result in the loss of access to computing resources. Users may be held accountable for their

conduct under any applicable AVC policies, procedures or collective bargaining agreements, as well as federal, state and local laws. Complaints alleging misuse of ITS resources will be directed to the appropriate supervisor or administrator.

- 5.4 Reproduction or distribution of copyrighted works, including, but not limited to images, text or software, without permission of the owner is an infringement of [U.S. Copyright Law](#) and is subject to civil damages and criminal penalties, including fines and imprisonment. Intentional violations of copyright law are federal crimes. Additionally, there may be liability for monetary damages for violation of copyright or breach of a license agreement. Therefore, unauthorized software copying is a serious matter. Also, much of what is published on the Internet (text and images) is subject to the same copyright law.
- 5.5 All computer and information technology equipment, including software and data communication links owned by AVC, is technically government property. As such, its use is subject to all constitutional and statutory controls and prohibitions pertaining to governmental conduct (for example prohibition against unreasonable searches).

## **6. Appropriate Use**

- 6.1 AVC's computing facilities and network systems exist to support the educational and public service mission of the college and the administrative functions that support this mission.
- 6.2 In general, the same guidelines that apply to the use of all college facilities apply to the use of the college's computing facilities.

## **7. Examples of Inappropriate Use**

Examples of misuse include but are not limited to the activities in the following list:

- 7.1 Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account holder.
- 7.2 Using the campus network to gain unauthorized access to any computer systems or information.
- 7.3 Knowingly performing an act that will interfere with the normal operation of computers, terminals, peripherals or networks.
- 7.4 Knowingly running or installing on any computer system or network or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses and worms.
- 7.5 Attempting to circumvent data protection schemes or uncover security loopholes.

- 7.6 Violating terms of applicable licensing agreements.
- 7.7 Using electronic mail to harass others.
- 7.8 Masking the identity of an account or machine.
- 7.9 Posting materials on electronic bulletin boards that violate existing laws or AVC policies.
- 7.10 Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing or deleting another user's files or software without the explicit agreement of the owner.
- 7.11 Using AVC resources for commercial purposes or for personal financial gain.
- 7.12 Using AVC resources for creation or distribution of unauthorized promotional materials or other forms of solicitation.

Activities will not be considered misuse when authorized by appropriate college officials for security or performance testing.

## **8. Enforcement**

- 8.1 Individuals may report suspected violations of these guidelines to an AVC supervisor, faculty member or administrator as appropriate. Reports of violations that are received by ITS will be forwarded to the appropriate supervisor or administrator.
- 8.2 Disciplinary action may be taken in accordance with one or more of the following: AVC policies, California law or the laws of the United States.
- 8.3 Minor infractions of these guidelines or those that appear accidental in nature are typically handled internally by the appropriate supervisor or administrator, in consultation with ITS. In some situations it may be necessary, however, to suspend account or computer access to prevent ongoing misuse while the situation is under investigation.
- 8.4 More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of college policies or repeated violations of minor infractions may result in the temporary or permanent loss of access to computing facilities.
- 8.5 Offenses that are clearly in violation of local, state or federal laws will result in the immediate loss of access to computing resources and will be reported to the appropriate law enforcement authorities. In addition, disciplinary action, up to and



including dismissal, may be applicable under other AVC policies, guidelines or collective bargaining agreements.

**9. Procedure for Review**

9.1 As the campus technology environment evolves, changes to these guidelines may become necessary.

9.2 The Information Technology Committee will solicit and review input from the campus community each year with regard to potential revisions to the guidelines.

9.3 Changes in the guidelines may be made by the Information Technology Committee in consultation with constituent groups and subsequently forwarded to the College Coordinating Council to be approved for recommendation to the college president.

## **Part Two: E-mail Use Highlights**

### A Quick Guide to using Antelope Valley College Electronic Mail

This is a summary. Please refer to Part Three for the more detailed guidelines governing the use of college electronic mail. The guidelines in Part Three apply to (1) all electronic mail services provided by the college, (2) all users and uses of such services and (3) all college records in the form of electronic mail, whether in the possession of college employees or other users of electronic mail services provided by the college.

#### **CAUTIONS**

E-mail may be subject to disclosure under the California Public Records Act.

The college may access or disclose the contents of your e-mail under specified circumstances described in these guidelines.

Information Technology Services staff might inadvertently see the contents of e-mail messages in the course of their duties.

Information Technology Services might have copies of e-mail on a back-up system even after you have discarded the messages.

Back-up copies might be retained for periods of time and in locations unknown to senders and recipients.

The security and confidentiality of e-mail cannot be guaranteed. Password protections are not foolproof.

It is possible for senders of e-mail to mask their identity.

Recipients are able to forward your e-mail without your knowledge or consent.

The contents of forwarded messages can be changed from the original.

Policy violations may result in serious consequences including but not limited to restriction of access to college computing facilities.

The California Penal Code makes certain computer crimes felony offenses.

Your college e-mail address is owned by Antelope Valley College District.

#### **DO**

Think twice before you click on the "send" button.

Comply with college policies and state and federal laws that apply to e-mail.

Protect the confidentiality of information you encounter inadvertently in e-mail or other records.

Respect the privacy of other people's e-mail.

Use personal and professional courtesy and considerations in e-mail.

Employ protections such as passwords to deter potential intruders.

Check with the sender if there is any doubt about the authenticity of a message.

Request information on e-mail back-up practices from Information Technology Services.

Ask a faculty member or supervisor for advice if you are not sure what these guidelines or college policies allow.

**DO NOT**

Violate law and college policy by theft or abuse of facilities or resources.

Seek out, use or disclose personal or confidential information unless authorized.

Access or disclose other people's e-mail without prior consent.

Knowingly interfere with other people's use of e-mail.

Send chain letters, "junk mail" or unsolicited advertising messages that are unrelated to the educational mission of the college.

Send messages urging the support or defeat of any ballot measure or political candidate.

Knowingly disrupt college electronic mail and other information technology services.

Use e-mail for unlawful activities or commercial purposes.

Use e-mail in violation of other college policies (such as harassment policies).

Use e-mail to give the impression that you represent the college (unless authorized to do so).

Let personal use of e-mail interfere with your employment or other obligations to the college.

Increase costs to the college by excessive personal use of e-mail.

Rely exclusively on electronic mail for purposes of archiving and record retention.

## Part Three: Complete Electronic Mail Guidelines

### 10. Introduction

These guidelines clarify the applicability of law and of other college policies to electronic mail. They also define procedures where existing policies do not specifically address issues particular to the use of electronic mail.

The college encourages the use of electronic mail and respects the privacy of users. It does not inspect, monitor or disclose electronic mail without the holder's consent except as noted in Section 4.4.

Users should be aware of the following:

10.1 Both the nature of electronic mail and the public character of the college's business make electronic mail less private than users might anticipate. For example, electronic mail intended for one person sometimes might be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or "listserver" intended only for the originator of the message might be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it might persist on backup facilities and thus be subject to disclosure under the provisions of Section 4 of these guidelines. The college cannot routinely protect users against such eventualities.

10.2 Electronic mail, whether or not created or stored on college equipment, may constitute a college record subject to disclosure under the [California Public Records Act](#) or other laws or as a result of litigation. The college evaluates all such disclosure requests against the precise provisions of the Act, other laws concerning disclosure and privacy or other applicable law.

Users of college electronic mail services also should be aware that the [California Public Records Act](#) and other similar laws jeopardize the ability of the college to guarantee complete protection of personal electronic mail resident (see Section 13.1.8) on college facilities.

The [California Public Records Act](#) does not, in general, apply to students except in their capacity, if any, as employees or agents of the college. This exemption does not, however, exclude student e-mail from other aspects of these guidelines.

10.3 The college, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the college, in general, protect users from receiving electronic mail they might find offensive. Members of the college community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

10.4 There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of these guidelines, for senders to disguise their identity. Furthermore, electronic mail that is forwarded might also be modified. Authentication technology is not widely and systematically in use at the college as of the date of these guidelines. As with print documents, in case of doubt, receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

10.5 Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of these guidelines. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of college policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.

## **11. Purpose**

The purpose of these guidelines is to assure that:

- 11.1 The college community is informed about the applicability of policies and laws to electronic mail;
- 11.2 Electronic mail services are used in compliance with those policies and laws;
- 11.3 Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and
- 11.4 Disruptions to college electronic mail and other services and activities are minimized.

## **12. Scope**

These guidelines apply to:

- \* All electronic mail systems and services provided or owned by the college; and
- \* All users, holders and uses of college e-mail services; and
- \* All college e-mail records in the possession of college employees or other e-mail users of electronic mail services provided by the college.

These guidelines apply only to electronic mail in its electronic form. The guidelines do not apply to printed copies of electronic mail. Other college policies however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either

their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

These guidelines apply equally to transactional information (such as e-mail headers, summaries, addresses and addressees) associated with e-mail records as they do to the contents of those records.

These guidelines are effective immediately.

### **13. Specific Provisions**

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

13.1.1 Purpose. Electronic mail services are to be provided by college organizational units in support of the educational mission of the college and the administrative functions that support this mission.

13.1.2 Users. Users of college electronic mail services are to be limited primarily to college students, employees, board members and members of associated groups or individuals for purposes that conform to the requirements of this section.

13.1.3 Non-Competition. College electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the college.

13.1.4 Restrictions. College electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the college; personal financial gain; personal use inconsistent with Section 13.1.8; or uses that violate other college policies or guidelines. The latter include, but are not limited to, college policies and guidelines regarding intellectual property or regarding sexual or other forms of harassment.

13.1.5 Representation. Electronic mail users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the college or any unit of the college 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 the college. An appropriate disclaimer is: "These statements are my own, not those of the Antelope Valley College District."

13.1.6 False Identity. College e-mail users shall not employ a false identity. E-mail might, however, be sent anonymously provided this does not violate any law or these guidelines or any college policy and does not unreasonably interfere with the administrative business of the college. An example of such anonymous e-mail would be e-mail sent by a system administrator using the postmaster account.

13.1.7 Interference. College 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: (i) send or forward e-mail chain letters; (ii) "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 (iii) "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.

13.1.8 Personal Use. College electronic mail services may be used for personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the college operation of computing facilities or electronic mail services; (ii) burden the college with incremental cost; or (iii) interfere with the e-mail user's employment or other obligations to the college. E-mail records arising from such personal use may, however, be subject to the presumption in Section 2, definition of a college e-mail record, regarding personal and other e-mail records. E-mail users should assess the implications of this presumption in their decision to use college electronic mail services for personal purposes.

## 13.2 Security and Confidentiality

13.2.1 The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including these guidelines, 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.

13.2.2 Board Policies governing confidential materials and communications prohibit college employees from disclosure of confidential information. This prohibition applies to e-mail records.

13.2.3 Notwithstanding the previous paragraph, 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 college e-mail services and on these and other occasions might inadvertently see the contents of e-mail messages. Except as provided elsewhere in these guidelines,

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 might 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 shall be accompanied by notification to the recipient that the e-mail has been inspected for such purposes.

13.2.4 The college attempts to provide secure and reliable e-mail services. Operators of college 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.

13.2.5 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 might be back-up copies that can be retrieved. Systems might 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 results in the copying of data onto storage media that might be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of e-mail vary from system to system. Electronic mail users may request information on the back-up practices followed by Information Technology Services (the operators of college electronic mail services) and Information Technology Services is required to provide such information upon request.

### 13.3 Archiving and Retention

College records management policies do not distinguish among media with regard to the definition of college records. As such, electronic mail records are subject to these policies.

The college does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section 13.2.5), if at all, only to assure system integrity and reliability, not to provide for future



retrieval, although back-ups may at times serve the latter purpose incidentally. Information Technology Services is not required by these guidelines to retrieve e-mail from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

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 embracing 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 Section 10.4), it is difficult to guarantee that e-mail documents have not been altered, intentionally or inadvertently.

E-mail users and those in possession of college 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 acid-free paper or microfilm, where long-term accessibility is an issue.

#### **14. Policy Violations**

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

#### **15. Responsibility for Guidelines**

The director of Information Technology Services is responsible for development and maintenance of these guidelines for issuance by the president.

#### **16. College Responsibilities and Discretions**

16.1 Information Technology Services will implement these guidelines and communicate these provisions to all users of college electronic mail services.

16.2 E-mail addresses will be published as directory information, subject to the same policies provided for other forms of directories maintained by the college.

16.3 Generally, a user's e-mail account(s) will be deleted once that individual's affiliation with the college is terminated. However, the college may elect to terminate the individual's e-mail account, redirect electronic mail or continue the account, subject to the provisions of Section 13.1 of these guidelines.

16.4 The Information Technology Services Department shall establish appropriate notification procedures regarding these guidelines to all e-mail users. New users shall positively acknowledge receipt and understanding of the policy. Such notification and acknowledgment may be electronic to the extent that the e-mail user's identity can be assured. It is recognized that it may not be possible to phase in such procedures immediately; however, the lack of comprehensive procedures shall not, in the interim, invalidate the provisions and applicability of these guidelines.

## **Appendix A: Privacy and Public Records Issues**

### **1. California Information Practices Act**

The California Information Practices Act guarantees individuals access to personal files maintained on them, with certain limitations and sets forth provisions to govern the collection, maintenance, accuracy, dissemination and disclosure of information about them. Special procedures for providing access to and protecting the privacy of college records containing personal data are required by the Information Practices Act.

### **2. California Public Records Act**

The California Public Records Act provides that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this State; that upon request public records must be available to public inspection within a reasonable time; and that every citizen has the right to inspect any public records except as provided in the Act. Refer to Section 320-23 for information regarding disclosure of information from public records.

### **3. Federal Privacy Act of 1974**

The Federal Privacy Act is designed to safeguard the rights and privacy of individuals from the encroachments of Federal agencies in maintaining records on individuals.

### **4. Fourth Amendment to the United States Constitution**

The Fourth Amendment protects the “right of the people to be secure in their persons, houses, papers and effect, against unreasonable seizures...” (Applied to State entities by the 14th Amendment.) Violation depends on expectancy of privacy. Courts have tended to hold that employees do not have a reasonable expectation of privacy in the e-mail messages sent on an employer’s e-mail system.

### **5. California Constitution, Article 1**

Article 1 of the California Constitution guarantees the right to privacy as an inalienable right, applicable to both public and private employees. As noted in 4 above, however, the courts have tended to hold that employees do not have a reasonable expectation of privacy with regard to e-mail.

### **6. The Electronic Communications Privacy Act (ECPA)**

The ECPA prohibits intentional, unauthorized accessing, interception or disclosure of electronic communications and protects electronic communication systems from outside intruders or “hackers” making unauthorized attempts to intercept or eavesdrop on information. The Act also provides that either party to the communication may intercept the communication for purposes of protecting business property from damage or to provide service and a party may give prior consent to interception of the communication.

Antelope Valley College prohibits discrimination and harassment based on sex, gender, race, color, religion, national origin or ancestry, age, disability, marital status, sexual orientation, cancer-related medical condition or genetic predisposition. Upon request we will consider reasonable accommodation to permit individuals with protected disabilities to (a) complete the employment or admission process, (b) perform essential job functions, (c) enjoy benefits and privileges of similarly-situated individuals without disabilities and (d) participate in instruction, programs, services, activities or events.

Send your comments regarding this document to any representative of the Information Technology Committee or to the Director of Information Technology Services at 3041 West Avenue K, Lancaster, CA 93536.

**Antelope Valley College**

**Board of Trustees**

Mr. Steve Buffalo

Mr. Steve Fox

Mr. Jack Seefus

Mrs. Betty J. Wienke

Mr. Earl J. Wilson

Ms. Harmony Perkins, Student Trustee