Draft 11 – Revised 05/7/09

Section x	**ITS Policies**	mm/dd/yy	-Effective
		05/17/2009	-Revised
Policy x.xx	**E-mail Policy**	Information Services	-Author

1. E-MAIL USE POLICY

1.1. Introduction

Electronic mail (e-mail) is available to facilitate the professional and business work of persons employed at Amarillo College (AC). It provides a way to communicate with individuals and with designated groups. AC encourages appropriate use of e-mail to enhance productivity through the efficient exchange of information in furtherance of education, public service, and the expression of ideas. Use of this resource must be consistent with these concepts. As a responsible member of the college community, employees are expected to act in accordance with the following policies. These policies are not all-inclusive and are subject to change. Generally accepted practices of common sense, decency, civility, and legality should be taken into account when e-mail is utilized. AC information resources are strategic assets that must be managed as valuable resources. Thus, this policy is established to achieve the following:

- To ensure compliance with applicable policies, statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of e-mail.
- To educate individuals using e-mail with respect to their responsibilities associated with such use.

1.2. Purpose

The Information Technology Service (ITS) staff is charged with maintaining the hardware, software, and network for maximum efficiency of the e-mail system. The purpose of the AC E-mail Policy is to establish the rules for the use of any AC e-mail system for the sending, receiving, or storing of electronic mail.

1.3. Audience

The AC E-mail Policy applies equally to all individuals granted access privileges to any AC information resource with the capacity to send, receive, or store electronic mail.

1.4. Definitions

1.4.1. **Electronic mail system**: Any computer software application that allows electronic mail to be communicated from one computing system to another.

1.4.2. **Electronic mail (e-mail):** Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

1.4.3. "**Mass e-mailings**" are considered those sent to a group (e.g., the entire campus or subsets, the student body subsets, programs, or external entities).

1.4.4. Encryption: Using different methods of hiding data transmission with secret code which can only be opened with a secret key or password.

1.4.5. **Archiving**: a packaging of files into one in order to copy onto media for permanent storage or to free space on local storage.

1.4.6. **Retention**: a policy that provides guidelines on how and when an organization should store, retain, and destroy e-mail or instant messages for compliance reasons.

1.4.7. **Spam**: unsolicited e-mail sent to a large number of addresses via the Internet.

1.4.8. **Phishing:** a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly.

1.4.9. **Black-list:** a list of persons or Internet sites who are disapproved of or are to be punished, boycotted, or blocked by other Internet sites.

1.4.10. **Incidental Use:** Incidental use includes activities not directly related to AC business, academics, or research. Examples of appropriate incidental use include access to non-AC e-mail accounts, social networking, search engines, and general informational websites.

1.4.11. **Confidential information** requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of AC to accomplish its mission as well as records about individuals requiring protection under the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA). Confidential information includes, for example, social security numbers, student financial aid information, salary and benefits information, alumni gifts, and student records.

1.4.12. **Sensitive information** requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to AC. It is assumed that all output is classified as sensitive unless otherwise indicated. Sensitive information includes, for example, class lists, contract data, and vendor data information.

1.4.13. **Public Information** can be made generally available both within and beyond AC. It should be understood that any information that is disseminated within the campus community is potentially available to the public at large in accordance with the Texas Open Records Act and the Freedom of Information Act (FOIA). Public information includes, for example, telephone directory information.

1.4.14. **Inappropriate/Prohibited Use:** These activities include, but are not limited to:

- Actions that compromise the integrity or security of any computer system (hacking).
- Commercial use (for personal profit).
- Criminal speech and/or speech or use, in the course of committing a crime - e.g., threats to persons, instructions on breaking into computer systems, child pornography, drug dealing, gang activity, etc.
- Offensive or disruptive activity such as inappropriate language, video, or graphics – obscene, profane, lewd, vulgar, disrespectful, threatening, or inflammatory language; harassment; personal attacks, including prejudicial or discriminatory attacks; or false or defamatory material about a person or organization.
- Dangerous information – information that if acted upon, could cause damage or present a danger of educational or business operation disruption.
- Violations of privacy – revealing personal information about others.
- Activities that involve pornographic material – electronic and print material which, by their design, are salacious, lascivious, lecherous, lustful, or demeaning to humans in their portrayal of aberrant sexual behavior.

1.4.15. The distribution of a computer virus or engagement in any procedure that interferes with the normal operation and delivery of services over the network.

1.5. Privacy

Electronic files created, sent, received, or stored on AC ITS information resources owned, leased, administered, or otherwise under the custody and control of AC are not private and may be accessed by authorized AC employees at any time without knowledge of the user. Employees have no expectations of privacy pertaining to electronic activity on any AC information resource. Electronic file content may be accessed by appropriate personnel (e.g., Human Resources, supervisors, ITS employees) in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resources Standards.

1.6. Policy Statements

1.6.1. Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents. The user should identify himself or herself clearly and accurately in all electronic communications. A user's concealing or misrepresenting identity or affiliation is inappropriate**.**

1.6.2. Alteration of the source of electronic mail or its message is unethical and illegal. Such action could cause AC to be blacklisted on a spam watch list.

1.6.3. Electronic mail is the property of the college; however, no attempt to access another's electronic mail by unauthorized individuals is permitted. ITS employees may, from time to time, have a need to access a user's e-mail for routine purposes of repair, upgrades, etc.

1.6.4. Concerning the issue of the federal law governing privacy, network system administrators will not intentionally access the content of e-mail messages, and if content is accidentally accessed, it will be treated as confidential.

1.6.5. The user is asked to be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent unauthorized access to its files. The college will be unable to guarantee absolute privacy and confidentiality of electronic documents. Password security and confidentiality are the responsibility of the user. ITS will provide guidelines for the frequency of change and the nature of passwords. In keeping with good judgment, users should create electronic documents as if they were to be made available to the public**.**

1.6.6. Abusive, threatening, or harassing e-mail is prohibited. While debate on controversial issues is inevitable and essential at an educational institution, e-mail of a debate nature should advance the cause of learning and mutual understanding.

1.6.7. The user is expected to promote efficient use of network resources consistent with the instructional, research, public service, and administrative goals of the college. The user is expected to refrain from any use that would interfere with another's work or disrupt network resources.

1.6.7.1. Access to the **Everyone Group** or sending an e-mail to the entire AC community is restricted to President's Cabinet level administrators or their designees.

1.6.7.2. The user is not to use the **Everyone Group** to send recipes, jokes or humor, large attachments, requests for placement of a pet, distribution of any form of spam, or any non-college related announcement.

1.6.8. The e-mail system is to be used for AC-related business with limited incidental use. The user should avoid wasteful and disruptive practices such as allowing large amounts of e-mail to go unattended, spreading chain letters, or sending other unsolicited material.

1.6.9. E-mail may not be used for commercial purposes unrelated to AC or for personal financial gain.

1.6.10. Standards of conduct expected of students, faculty, and staff in regard to the use of telephones, libraries, and other institutional resources apply to e-mail. Users will be held accountable for their actions, as they would be when using other forms of communication.

1.6.11. Individuals must not send or forward confidential or sensitive AC information through non-AC e-mail accounts. Examples of non-AC e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e-mail provided by other Internet Service Providers (ISP).

1.6.12. Sending Mass E-mailings to Students: The purpose of this policy is to provide guidance on the appropriate use of mass e-mailings to the student population. For the purposes of this policy, "mass e-mailings" are considered those sent to the entire student body or a subset of students larger than a department, program, or satellite campus. This policy does not limit the right of individual faculty members, departments, programs, or satellite campus directors to send e-mails to their respective constituencies nor does it limit the right of the College Relations Office to use prospective student e-mail addresses for marketing and recruitment purposes.

1.6.12.1. All requests for student e-mail address extracts from the student database must be initiated through the Registrar.

1.6.12.2. Mass e-mailings are an internal form of communication to be used for official academic and administrative purposes only. The sale/distribution of AC student e-mail addresses to non-AC entities is prohibited, except as allowed by FERPA and HIPAA regulations. In such cases where distribution is allowed, the request must be fulfilled by the Registrar's office.

1.6.12.3. E-mail recipient lists should be placed in the 'blind copy' (BC) field to prevent e-mail address harvesting.

1.6.12.4. E-mail addresses extracted for purposes of mass e-mailings may only be used by officially designated "Gatekeepers" - individuals assigned responsibility to approve mass e-mailings for certain student populations as described below.

1.6.12.4.1. The contents of e-mails for mass distribution must have written approval (e-mailed approvals suffice) from the appropriate gatekeeper (described below).

1.6.12.4.1.1. Academic mass e-mailings to the entire student body or a subset greater than the Division level must have the approval of the Vice President and Dean of Instruction (or designee).

1.6.12.4.1.2. Academic mass e-mailings to a subset of students at the Division level must have the approval of the appropriate Division Chair (or designee).

1.6.12.4.1.3. Administrative mass e-mailings to students must have the approval of the Dean of Enrollment Services (or designee) regardless of the student population targeted.

1.6.12.4.1.4. Recruitment-oriented mass e-mailings to prospective students must have the approval of Enrollment Services (or designee), regardless of the size of the population targeted.

1.6.12.4.2. Examples of appropriate mass e-mails to all students: Issues involving College facilities or affecting working/teaching conditions, such as power outages or building closures; essential or urgent official administrative e-mail from College departments, such as financial aid and registration information, policy and procedure dissemination, and technology updates.

1.6.12.4.3. Examples of inappropriate mass e-mails to all students: For personal gain or unlawful purposes; from an individual rather than a College department; optional student event announcements; chain letters; general broadcast messages or announcements (clubs, student government, intramural events, theater); for unlawful purposes; containing information of a confidential or sensitive nature; promotion of political viewpoints; surveys that do not serve sanctioned College purposes; messages containing confidential information such as course grades, financial aid award amounts, or tuition/fee payment amounts; sending a mass e-mailing on the behalf of a non-AC entity.

1.7. Guidelines and Standard Operating Procedures (SOP)

1.7.1. Examples of Appropriate Uses of E-mail: Sharing information or collaborating with peers concerning college related business.

1.7.2. Examples of Inappropriate Uses of E-mail:

1.7.2.1. Announcement of the sale of personal property or the solicitation of support for a particular political position.

1.7.2.2. Work related automated information delivery from external sources such as listservs or RSS feeds is acceptable. The user is expected to confine subscriptions to a limited number and not backlog the E-mail system with a large number of items.

1.7.2.3. Since numerous methods for shaping large attachments are available, sending large attachments (such as photos, .pdf files, or other files over 1 MB) is prohibited. Users who need to send large files can consult with ITS staff for recommendations.

1.7.3. General Guidelines

1.7.3.1. The user is expected to be honest, legal, and ethical and consider the implications of the message sent.

1.7.3.2. Keep messages simple and direct.

1.7.3.3. Do not include confidential or sensitive information (e.g., social security numbers, home addresses, and other information covered by FERPA and HIPAA).

1.7.3.4. Send any/all mass e-mail messages to the sender with all recipients placed in the BCC (Blind Courtesy Copy) field. This protects against the harvesting of e-mail addresses and makes the message easier to print.

1.7.3.5. Include sender's phone number/extension.

1.7.3.6. Senders of mass e-mail are encouraged to examine, with assistance, a draft version of the message to make sure the content and grammar meet professional communication standards.

1.7.3.7. When an e-mail message is to be sent to more than 1,000 recipients, send separate mailings in groups of no more than 1,000 e-mail addresses.

1.7.4 General Procedures

1.7.4.1 Supervisors may request a network and/or e-mail account for new full-time employees by completing the online Employee Access Request Form. The completed form should be signed by the employee's supervisor and submitted to ITS. (https://acs.actx.edu/forms/access_request.htm)

1.7.4.2 Supervisors may request a network and/or e-mail account for new part-time employees by completing the online Employee Access Request Form. The completed form should be signed by the employee's supervisor and submitted to ITS. (https://acs.actx.edu/forms/access_request.htm)

1.7.4.3 At the beginning of each semester, e-mail accounts will be created for part-time faculty whose supervisor did not request an account be created for them.

1.7.4.3.1 ITS will extract names from academic faculty class assignments in Datatel two weeks prior to the beginning of each semester and two weeks after the beginning of each semester to determine which faculty (part time and full time) do not have e-mail accounts. E-mail accounts will be created for those who do not have one.

1.7.4.3.2 Once created, the ITS staff will inform the supervisors to notify the new or reinstated part-time faculty about the e-mail account. Currently, Outlook serves as the official AC communication mechanism and should be frequently checked for institutional announcements and information.

1.7.4.4 At the beginning of each fiscal quarter, e-mail accounts will be created for full-time and part-time employees whose supervisor did not request an account be created for them.

1.7.4.4.1 ITS will extract names from Human Resources (HR) payroll records to determine active employment. E-mail accounts will be created for those employees who do not have an account.

1.7.4.4.2 Once created, the ITS staff will inform supervisors to notify the new or reinstated employee about the e-mail account. Currently, Outlook serves as the official AC communication mechanism and should be frequently checked for institutional announcements and information.

1.7.4.5 E-mail accounts for faculty, classified employees, and administrators are disabled on the last day of employment unless ITS is notified otherwise by Human Resources.

1.7.4.6 Part-time academic faculty e-mail accounts will remain active until HR records indicate they have received no salary for 90 days.

1.7.4.6.1 A list of part-time faculty who have not been paid for 90 days will be developed by ITS each semester. The supervisors of those faculty will receive a list of those names and be informed that those on the list are marked for removal from the AC e-mail system. To accommodate long-term part-time faculty in good standing, supervisors can verify to ITS their plans to continue employment of individuals, and their accounts will not be disabled. This verification from the supervisor will be required each semester.

1.7.4.6.2 It is the responsibility of department chairs or coordinators to notify ITS at the end of a semester if they do not plan to have a part-time faculty member return. The accounts of those part-time faculty members will be disabled or deleted.

1.7.4.7 Supervisors have the authority to have the e-mail account of one of their employees disabled at any time when working through HR to notify ITS.

1.7.4.8 Since e-mail storage space is a finite resource, users will use the allocated storage space efficiently and adhere to the records management policies in their area.

1.7.4.9 Requests for additional storage space in Outlook must be reviewed and approved by the requester's supervisor and ITS to determine additional needs.

1.7.5 Disclaimers

1.7.5.3 (Should be 1.7.5.1) AC's enterprise e-mail system will attach the following disclaimer to any "sent" e-mail having an e-mail address external to the AC e-mail system

Any views or opinions expressed in this e-mail are solely those of the author and do not necessarily represent those of Amarillo College. This e-mail and its attachments may be confidential and are intended for the person to whom the e-mail is addressed. If you are not the intended recipient, you must take no action based on it, nor must you copy or distribute the information. Please contact the sender if you believe you have received this e-mail in error. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Amarillo College, therefore, does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission.

1.7.5.4 (Should be 1.7.5.2) AC's enterprise e-mail system will attach the following disclaimer to any "sent" e-mail having an e-mail address internal to the AC e-mail system.

* This message is intended only for [recipient name]. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

* Employees of Amarillo College are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by e-mail communications. Any such communication is contrary to college policy and outside the scope of the employment of the individual concerned. The college will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising. Employees who receive such an e-mail must notify their supervisor immediately. AC college e-mail policy is available here (*insert link to e-mail policy*).

1.7.6 Amarillo College will develop an e-mail retention policy. A group will be established to develop that policy, working with AC Records Management personnel. When the policy is developed, this document will be updated to include the policy.

1.7.7 Amarillo College will implement technology to encrypt e-mail for those departments that routinely send sensitive information. The departments currently identified are: Business Office, Financial Aid, Human Resources, and Registrar. Other departments may be identified and included in encryption procedures.

1.8. Disciplinary Actions ***(this section may move to a different section of the manual)***

1.9. References

Copyright Law of the United States
http://www.copyright.gov/title17/

Foreign Corrupt Practices Act (FCPA)
http://www.usdoj.gov/criminal/fraud/fcpa/

Prosecuting Intellectual Property Crimes
http://www.usdoj.gov/criminal/cybercrime/ipmanual/index.html

Federal Information Security Management Act (FISMA) Implementation Project
http://csrc.nist.gov/groups/SMA/fisma/index.html

The Health Insurance Portability and Accountability Act
http://www.hhs.gov/ocr/hipaa/

The Public Information Act (Texas Government Code, Chapter 552)
http://www.tsl.state.tx.us/agency/customer/pia.html

State Records Management Laws, State Agency Bulletin Number Four
http://www.tsl.state.tx.us/slrm/recordspubs/stbull04.html

Texas Administrative Code, Chapter 202 (Information Security Standards)
http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202

Information Resources Management Act (IRMA) (TEX.GOV'T CODE Â§ 2054)
http://www.dir.state.tx.us/oversight/

Practices for Protecting Information Resources Assets (State of Texas, Department of Information Resources)
http://www.dir.state.tx.us/IRAPC/practices/index.htm

Standards Review and Recommendations Publications (SRRPUB) (State of Texas, Department of Information Resources)
http://www.dir.state.tx.us/standards/

Homeland Security Act
http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm

http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html