Under IT Council Review (April 2009)

Section 2	**Information Technology Services**	mm/dd/yy -Effective
		4/13/09 -Revised
Policy 2.1 - 2.10	**Internet Use Policy**	ITS -Author

2. INTERNET USE

2.1. Introduction

Information resources are strategic assets of Amarillo College (AC) 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 the Internet.
- To educate individuals who may use the Internet, the intranet, or both with respect to their responsibilities associated with such use.

2.2. Purpose

To fulfill AC's mission, AC provides access to a broad range of information resources, including those available through the Internet. We make this service available as part of our mission to offer a broadly defined program of informational, educational, recreational and cultural enrichment opportunities for the members of the College and regional community. AC only assumes responsibility for the information residing on AC's server network and/or through authorized services. The Internet offers access to many valuable local, national, and international sources of information. However, not all sources on the Internet provide accurate, complete, or current information. A good information consumer evaluates the validity of information found.

2.3. Audience

The AC Internet Use Policy applies equally to all individuals granted access to any AC information resource with the capacity to access the Internet, the intranet, or both. This includes all employees and students. If you have any questions about this policy, please contact Information Technology Services (ITS) personnel for more information clarification.

2.4. Definitions

2.4.1. **User**: An individual, automated application or process that is authorized to access the resource by AC, in accordance with AC's procedures and rules.

2.4.2. **IT resources**: Any and all technology-based systems owned by or licensed to AC that are capable of creating, printing, storing, and displaying information and used to perform AC work. This includes computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology, telecommunication resources, network environments, telephones, fax machines, printers, wireless antennae, smart classroom and instructional devices such as projectors, document cameras, and DVD players). IT resources also includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

2.4.3. **Internet**: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

2.4.4. **Intranet:** A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access.

2.4.5. **World Wide Web:** A system of Internet hosts that supports documents formatted in HyperText Markup Language (HTML) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Microsoft Internet Explorer, Mozilla and Firefox.

2.4.6. **Vendor:** someone who exchanges goods or services for money.

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

2.4.8. **Patches:** Minor corrections or modifications to a computer program or application.

2.4.9. **Authentication:** Process used to prove authenticity of a network account.

2.4.10. **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 email accounts, social networking, search engines and general informational websites so long as they do not interfere with an employee's job performance, violate any other policies, or damage College property.

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

2.4.11.1. Actions that compromise the integrity or security of any computer system (hacking).

2.4.11.2. Commercial use (for personal profit).

2.4.11.3. 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.

2.4.11.4. 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.

2.4.11.5. Dangerous information – information that if acted upon, could cause damage or present a danger of educational or business operation disruption.

2.4.11.6. Violations of privacy – revealing personal information about others.

2.4.11.7. 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.

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

2.4.11.9. Illegal distribution, publication or copying of copyrighted materials.

2.5. Ownership

Electronic files created, sent, received, or stored on computers owned, leased, administered or otherwise under the custody and control of AC are the property of AC.

2.6. 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 expectation of privacy pertaining to electronic activity on any AC information resource. Electronic file content may be

accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

2.7. Policy

2.7.1. Responsibility of users - The user will engage in no activity, which abuses any resource of the AC network, whereby the network is restricted in use or is damaged in any manner.

2.7.2. The ITS staff constantly monitors the AC network to insure the proper operation of the service.

2.7.3. Access to the Internet is provided to authorized users primarily for business, academic and research use only. Incidental use (defined below) is permitted provided the activity does not interfere with the primary use.

2.7.4. All software used to browse the Internet must be part of the AC standard software suite or approved by the ITS. It is the responsibility of the end-user to assure any approved browser incorporates current security features and patches.

2.7.5. Any computer connecting to the AC network must have current anti-virus software installed.

2.7.6. All user activity on AC ITS resources are subject to logging and review.

2.7.7. Ultimate responsibility for content on all AC Web sites resides with College Relations.

2.7.8. Business related purchases over the Internet are subject to AC procurement rules.

2.7.9. No personal commercial advertising may be conducted via AC Web sites.

2.7.10. AC Internet access may not be used for personal gain or non-AC personal solicitations.

2.7.11. No sensitive AC data will be made available via AC Web sites without proper authorization.

2.7.12. All sensitive AC material transmitted over external networks must be encrypted and authenticated (e.g., email, FTP, VPN, etc.).

2.7.13. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

2.7.14. Incidental Use

2.7.14.1. Incidental personal use of Internet access is restricted to AC approved users; it does not extend to family members or other acquaintances.

2.7.14.2. Incidental use must not result in direct costs to AC.

2.7.14.3. Incidental use must not interfere with the normal performance of an employee's work duties.

2.7.14.4. No files or documents may be sent or received that may cause legal liability for, or embarrassment to, AC. For example, unacceptable incidental use includes using the AC Internet access to send spam, chain-letters, or unsolicited emails through off-site personal accounts.

2.7.14.5. Storage of personal files and documents within AC's ITS resources should be nominal. All files and documents – including personal files and documents- are owned by AC, may be subject to open records requests, and may be accessed in accordance with this policy.

2.8. Guidelines and Standard Operating Procedures

2.8.1. **Choosing and evaluating resources -** The Internet is a global entity with a highly diverse user population and information content. College patrons use it at their own risk. The College cannot censor access to materials or protect users from materials they may find offensive. The user alone is responsible for the information accessed through the Internet. The College reserves the right to choose the links that appear on the AC Website. In doing so, the College will provide links only to those sites that conform to the College's mission and goals. AC does not control information accessible through the Internet and does not accept responsibility for its content. AC is not responsible for changes in the content of the linked sources, nor for the content of sources accessed through secondary links. As with printed information, not all sources on the Internet provide accurate, complete, or current information. Users should evaluate Internet sources just as they do printed publications, questioning the validity of the information provided. The College expressly disclaims any liability or responsibilities arising from access to or use of information obtained through its electronic information systems or any consequences thereof.

2.9. Disciplinary Actions

Upon discovery of inappropriate Internet activity, ITS staff will notify the appropriate personnel or supervisor. Violations may result in a denial of access to College computer resources, and those disciplinary actions provided or authorized by the Rules and Regulations Policy Manual, employee handbooks, and Student Rights and Responsibilities of AC through the Office of Human Resources or Enrollment Management. Users will be held personally liable for any actions that violate copyright laws.

2.10. 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