Acceptable Use of Technology Resources

The American Indian College Acceptable Use Policy promotes the efficient, ethical, and lawful use of AIC's information technology resources. The College's computing systems, networks, and associated facilities are intended to support the College's mission and to enhance the educational environment. Any use of these resources deemed inconsistent with the mission and purpose of the College will be considered a violation of this policy.

Scope

This policy applies to anyone who uses the College's information technology (IT) resources. The resources covered by this policy include, but are not limited to computer hardware and software; electronic devices such as personal digital assistants (PDAs), smart phones, and cell phones; telephone and data networks; and electronically stored data. Use of these resources includes access from off campus and on campus, as well as access from privately owned computers and electronic devices.

Rights & Responsibilities

Access to and use of AIC IT resources and the Internet shall comply with federal laws, the laws of the State of Arizona, and the policies and procedures of the College. By using AIC's IT resources, all users agree to the rules, regulations, and guidelines contained in this Acceptable Use Policy.

Computers and networks provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a revocable privilege and requires that individual users behave ethically and act responsibly. This AUP is intended to supplement College Policy and does not release users from compliance with any existing policies that address ethical issues such as harassment, academic dishonesty, and plagiarism.

College-provided IT resources are primarily designated for instructional, research, or administrative purposes. Employees and students may use these resources for personal purposes as long as that use does not interfere with the primary use and does not interfere with an employee's normal duties and responsibilities.

The College's computers and networks are shared resources, for use by all employees and students. Any activity that inhibits or interferes with the use of these resources by others is not permitted. The College will ensure reasonable use by monitoring access logs, traffic data, and network utilization.

Users are responsible for all activities to and from their access accounts. Users must take every precaution to protect access accounts. Under no circumstances should a user allow someone else to share an access account.

Users should not assume or expect any right of privacy with respect to the College's IT resources. Although the College does not routinely monitor the communication of its employees or students, system administrators or other authorized college personnel may access or examine files or accounts that are suspected of unauthorized use or misuse, that have been corrupted or damaged, or that may threaten the integrity of the College's computer systems. In addition, files, e-mail, access logs, and any other electronic records may be subject to search under court order.

Prohibited Use of Information Technology Resources

It is a violation of this policy to:

1. Intentionally and without authorization, access, modify, damage, destroy, copy, disclose, print, or take possession of all or part of any computer, computer system, network, software, data file, program, database, or any other College IT resource. This includes:
    a. Gaining access by willfully exceeding the limits of authorization.
    b. Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means.
    c. Gaining access by using another person's name, password, access codes, or personal identification.

   d. Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes.
2. Give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or e-mail account, database, or any other College IT resource.
3. Load any third-party software on computer systems in the computer labs, unless authorized by a member of the lab staff, a faculty member, or an Information Technology Services (ITS) representative.
4. Transfer copyrighted materials to or from any system, or via the College network, without the express consent of the owner of the copyrighted material. (See section entitled "File Sharing and Copyright Infringement.").
5. Provide unauthorized external access to College-developed or commercially-obtained IT resources.
6. Use any College IT resource for commercial, political, or illegal purposes; personal financial gain; or harassment of any kind.
7. Display obscene, lewd, or otherwise offensive images or text.
8. Intentionally or negligently use computing resources in such a manner as to cause network congestion and performance degradation.

Private Computers Connected to the College Network

The following apply to anyone connecting a private computer to the College network via a wireless LAN connection, a dial-up network connection or any other network connection.

The owner of the computer is responsible for the behavior of all users on the computer, and all network traffic to and from the computer, whether or not the owner is aware of the traffic generated.

A private computer connected to the network may not be used to provide network access for anyone who is not authorized to use the College systems. The private computer may not be used as a router or bridge between the College network and external networks, such as those of an Internet Service Provider (ISP).

Should IT staff have any reason to believe that a private computer connected to the College network is using the resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and action will be taken with the appropriate authorities.

Any residential student with an authorized network account may it for scholarly purposes, for official College business, and for personal use, so long as the usage (1) does not violate any law, regulation, or this policy; (2) does not involve extraordinarily high utilization of College resources or substantially interfere with the performance of the College network; and (3) does not result in commercial gain or profit.

Users are responsible for the security and integrity of their personal systems. In cases where a computer is "hacked into," the user shall either shut down the system or remove it from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading.

The following types of servers should never be connected to the College network: DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses as well as RADIUS, LDAP, AD, or any other server that provides authentication services.

Electronic Mail

The College e-mail system is not a private secure communications medium. As such, e-mail users cannot expect privacy. By using the College e-mail system, each user acknowledges:

The use of electronic mail is a privilege not a right. Transmitting certain types of communications is expressly forbidden. This includes messages containing chain letters, pyramids, urban legends, and alarming hoaxes; vulgar, obscene, or sexually explicit language; threatening or offensive content; derogatory, defamatory, sexual, or other

harassment; and discriminatory communication of any kind. As with other information technology resources, the use of e-mail for commercial or political purposes is strictly prohibited.

Under the Electronic Communications Privacy Act, tampering with e-mail, interfering with the delivery of e-mail, and using e-mail for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.

E-mail messages should be transmitted only to those individuals who have a need to receive them. Distribution lists should be constructed and used carefully. E-mail distribution lists should be kept current and updated regularly. Inappropriate mass mailing is forbidden; this includes multiple mailings to newsgroups, mailing lists, or individuals (e.g., "spamming," "flooding," or "bombing").

All users of the College e-mail system waive any right to privacy in e-mail messages and consent to the access and disclosure of e-mail messages by authorized College personnel. Accordingly, the College reserves the right to access and disclose the contents of e-mail messages on a need-to-know basis. Users should recognize that under some circumstances, as a result of investigations, subpoenas, or lawsuits, the College might be required by law to disclose the contents of e-mail communications.

File Sharing and Copyright Infringement

Federal copyright law applies to all forms of information, including electronic communications. Members of the College community should be aware that copyright infringement includes the unauthorized copying, displaying, and/or distributing of copyrighted material. All such works, including those available electronically, should be considered protected by copyright law unless specifically stated otherwise.

American Indian College complies with all provisions of the Digital Millennium Copyright Act (DMCA). Any use of the American Indian College network, e-mail system, or website to transfer copyrighted material including, but not limited to, software, text, images, audio, and video is strictly prohibited. Therefore, the use of peer-to-peer file sharing programs such as BitTorrent, Kazaa, Morpheus, iMesh, etc. is, in most cases, a violation of College policy and federal law.

Anyone using College IT resources to commit acts of copyright infringement will be subject to the College's due process. Acts of piracy are violations of state and federal laws, and as such, may result in criminal charges. Suspected infringement of the DMCA should be reported to an AIC staff member.

Reporting Violations of IT Acceptable Use Regulations

Violations of this Acceptable Use Policy should be reported immediately to the Director of Technology, The College will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of these regulations will result in the appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, or expulsion from the College, and legal action.

Indemnification/Liability Statement

American Indian College makes absolutely no warranties of any kind, either express or implied, for the Internet services it provides. The College will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The College is not responsible for the accuracy or quality of information obtained through its Internet services, including e-mail. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

The user agrees to indemnify and hold harmless American Indian College, the Board of Regents, The Board of Administration and College employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the College's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.