Computing Services Policies
Appendix Listings

Appendix A: Approved Operating Systems for use at ASC

As of: 03/01/04

- Windows 2000 and XP are the campus standard for PCs at this time. Each version is fully supported when installed from a clone deployed by CS. Windows XP, based on the recommendation of CS staff may not be loaded based on the limitations of the computer being recloned.

- (original wording) Windows XP, on an approval basis, is supported at ASC. However, if Windows 2000 will handle the applications and tasks that are needed for the position, CS may decide not to install Windows XP on the computer.

- Windows 98 and earlier versions are NOT SUPPORTED.

- For Macintosh computers, all OS versions from OS 8.0 to OS 9.2.2 are supported.

- Macintosh OS 10 and higher can be installed and supported on a limited basis with approval from CS.
Appendix B: Approved and Supported Software

As of: 03/01/04

- Microsoft Office 2000 is the campus standard on PC’s at this time. It is fully supported when installed from a clone deployed by CS. Updates and upgrades to this software are supported.

- Microsoft Office XP is supported on an approval basis as determined by CS.

- Microsoft Office 97 is NOT SUPPORTED.

- Microsoft Office 98, 2000, 2002, and Office X for Macintosh are supported.

- Other software that comes installed on the basic clone from CS is supported.

- Software that is not installed on the campus clone, but is being run on roughly 10% of the machines on campus may be supported.

- Additional software may be added to the supported list if the CIO of CS gives written approval.
Appendix C: Supported Computer System Vendors

As of: 03/01/04

ASC maintains one central supported vendor to provide a campus standard for desktop computing. All computer purchases require an approval signature on the purchase requisition. The “approval signature” does not necessarily imply that the equipment is supported. Apple Macintosh computers purchased with the approval of CS that comply with the latest supported OS will also be supported.
**Appendix D:** Blacklisted unsupported software

As of: 03/01/04

- Kaza, Kaza Lite, Grokster, Limewire, Blubster, and other file/media sharing programs.
- Unauthorized virus scanning software that is not provided by the College.
- Software for which the user cannot provide documentation of a valid license to install and operate the software.
- Malicious (Malware) or Ad Propagating software (Adware).
- For more information on Copyright Infringement, please see Appendix #H, pg 80, below.
Appendix E: Account Request Form

As of: 03/01/04

Side 1 on page 76
Side 2 on page 77
# Account Request/Acceptable Use Policy Form

The purpose of this form is to request the creation, deletion, or modification of a computing account for campus network or Banner access. If you have any questions about this form, call Computing Services at x7741. Return the completed form to Computing Services.

## Requestor

<table>
<thead>
<tr>
<th>Name</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Job Title</th>
<th>ID #: (if you don't know your ID#, SSH can be substituted)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department</th>
<th>Room/Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telephone Number</th>
<th>Machine Type</th>
<th>PC:</th>
<th>Mac:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Signature:**

**Date:**

**BEFORE SIGNING:** It's important that you read the "Acceptable Use Policy Statement" on the back of this form. Your signature indicates that you will comply with the policy.

## Supervisor Approval

<table>
<thead>
<tr>
<th>Print Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Action

### Network and/or Banner Account

- [ ] Create New Account
  - Specify preferred login name.
  - You have the option of selecting your login name. It must include your last name (no hyphenated names allowed). A recommended login name would be first name_last name (e.g., robert.smith). You could use a nickname in place of your first name if you prefer. The login name is what you type in each time you log in to your network account and will also be the first part of your email address (example: bob_smith@adams.edu).

- [ ] Modify Existing Account

- [ ] Close Account
  - Closure of an account will remove access to the ASC network, email, web, disk and Banner

- [ ] Group Membership:
  - Please specify the name of the shared directory:

- [ ] Reassign Workstudy Acct.
  - Workstudy Login Name:

- [ ] Banner Account* (Note: When Banner Access is requested, we will send out an additional form for approval signatures.)

- [ ] Same Banner Access As:

## For CS Office Use Only

- New Novell and/or Banner Login:

- Entered in GOMAIL & PIN in GOMAPAD:

- Date Created:
Acceptable Use Policy

01.B. Purpose

• Information technology resources are central to the educational mission of Adams State College (ASC). All ASC students, faculty and staff are encouraged to use these resources, provided that they respect the rights of others, abide by all college policies and applicable state and federal laws, and assume shared responsibility for safeguarding the college's information technology environment.

• This policy, in conjunction with the ASC Electronic Communications Policy (policy 01.D, pg. 10), defines your responsibilities as a user of ASC computing and electronic communication resources. Although this policy attempts to address the most common situations that may arise, it's impossible to foresee every situation. Each user is trusted to use the network responsibly, whether or not there is a guideline addressing each possible situation. As a representative of ASC you are expected to respect the college's good name in your electronic dealings with those both within and outside of the college.

• The central principles that govern the acceptable use of college information technology resources can be summarized, as follows:

01.B.1. Usage Guidelines

01.B.1.a. Unethical - ASC's computing resources may not be used for any activity that is illegal, unethical, or contrary to the educational goal of the college.

01.B.1.b. Policy compliance - Students, faculty and staff must comply with the applicable college policies and state and federal laws when using college computing-resources.

01.B.1.c. Storage - The college’s information technology resources are limited and users must avoid storing or using programs that interfere with the proper functioning of the network or that unnecessarily burden network capacity.

01.B.1.d. Misconduct - Freedom of expression and the existence of an open environment conducive to inquiry and learning will be respected by the college with regard to the use of computing resources, however, behavior that constitutes misconduct will not be protected.

01.B.2. Institutional Purposes

• The use of computing and networking resources is for purposes related to ASC's mission of education, scholarship, and public service. Members of the ASC community may use computing and networking resources only for the purposes related to their studies, their instruction, the discharge of their duties as employees, their official business with the college, and their other college-sanctioned activities.

01.B.3. Account Access

01.B.3.a. Assigned Accounts - No person may use, or attempt to use, any computer accounts other than his/her own assigned account. The negligence of another user in revealing an account name and password does not confer authorization to use the account.

01.B.3.b. Lending - An account owner may not lend his/her account(s) to another user.

01.B.3.c. Accessing Files - A user should only access, or attempt to access, files in his/her own accounts, files which have been made available to him/her by the files' owner, or files which have been made publicly accessible by the files' owner. Hacking to discover other user's private information is unacceptable.

01.B.3.d. Activity - Each account owner is responsible for all computing activity involving that account and will be held liable for any misuse of that account.

01.B.3.e. Transferring authorization - The privilege of using ASC equipment, wiring, computer and network systems is provided by the college and may not be transferred or extended by members of the campus community to people or groups outside of the college, without proper authorization.

01.B.4. Proper Use of Computing Resources

01.B.4.a. Violating activities - Computing resources may not be used for any activity that violates state or federal laws. Such activities include, but are not limited to intimidating, threatening or harassing individuals, or violating the college's policies concerning relationships between college constituencies.

01.B.4.b. Money-making - College computing resources may not be used for money-making or commercial purposes.

01.B.4.c. Infringing Usage - Every user is expected to use the computing facilities in a manner which does not infringe upon use of those facilities by other people and which does not waste "soft" resources (e.g., computer time) or "hard" resources (e.g., paper, disk space, documentation materials). Examples would be the repeated transfer of large files that cause network congestion, game playing activity that "hogs" excessive bandwidth or the printing of multiple copies of large documents.

01.B.4.d. Storage of programs - No person may store or use programs on college-owned systems that violate or hamper another person's use of computing resources. Examples of such programs are ones that attempt to obtain another user's password, acquire another user's files, circumvent system security measures, crash the computer system, harass users, etc. The devising and/or spreading of computer viruses is expressly forbidden.

01.B.4.e. File Storage - Network resources have been allocated and installed to insure optimum performance. Changes are limited to areas to which the user has been granted explicit access, for example shared office or home directories. Users should manage their shared file space in a responsible manner. Users are also responsible for backup of data stored on the network or on an ASC owned machine that is being utilized.

01.B.4.f. Personal Hardware - Attaching personal hardware to the campus network without the express approval of CS is not allowed. Incompatible hardware can cause damage to the system and/or impact network performance.

01.B.5. Use of Licensed Software and Copyrighted Electronic Materials

01.B.5.a. Personal use - No user is allowed to store or use personal, private or departmental copies of licensed software (any software not provided by CS other than software explicitly identified as freeware or public domain) on any ASC computer system of network unless the user provides CS with copies of the license agreement for the software and proof of ownership or purchase. It will be that person's responsibility to assure that installation of personal or private copies complies with the provisions of the license agreement.

01.B.5.b. Stolen software - Stolen or bootleg copies of software are not allowed on any ASC computing system.

01.B.5.c. Copying software - No user may copy, or attempt to copy, any proprietary or licensed software provided or installed by CS.

01.B.6. Privacy Considerations

01.B.6.a. Individual users - Files, tapes, disks, e-mail, information programs and data owned by individual users should be considered private, whether or not the information is accessible by other users.

01.B.6.b. Tampering - Tampering with e-mail, interfering with or intercepting its delivery and using e-mail for criminal purposes may be felony offenses. The Electronic Communication Privacy Act places electronic mail in the same category as messages delivered by the US Postal Service.

01.B.6.c. Confidentiality - CS will maintain the confidentiality of all information stored on ASC computing resources. Similarly, each user is expected to maintain the confidentiality of all information stored on computing resources in his or her charge. There are times, however, where CS may access user accounts, as required, to protect the integrity of the computing system such as, in the case of files suspected of unauthorized use or misuse or that have been corrupted or damaged.

01.B.6.d. Disclosure - Requests for disclosure of confidential information will be governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and by the Colorado Open Records Law. All such requests will be honored only when approved college officials who are the legal custodians of the information requested, or when required by state or federal law, or by court order.

01.B.7. Suspension or Revocation of Access - Violations of this policy are dealt with seriously and will be handled in accordance with the procedures outlined in the ASC Student Handbook or ASC Institutional Handbook for Professional Personnel. Users suspected of violating these policies may be temporarily denied access to ASC's information technology resources during investigation of the alleged abuse. Illegal acts involving ASC information technology resources may also be subject to prosecution by state and federal authorities.
Appendix F: Volunteer Account Request Form

As of:
Appendix G: Exceptions

As of: 03/01/04

VIII.A.1. What are our approved exceptions (i.e. Print Shop, Financial Aid) and our process for approval of exceptions?

For policy #04.A
Appendix H: Digital Millennium Copyright Act

Background

In December of 1996, the United States took a leadership role in directing the World Intellectual Property Organization (WIPO), a unit of the United Nations, to legislate new treaties between member nations regarding intellectual property and copyright. Those treaties were based on the Berne Convention of 1971. In October of 1998, congress gave its approval to the Digital Millennium Copyright Act (DMCA) as an implementation of our obligation under those treaties. Although the DMCA was intended as the implementation of the WIPO treaties, its reach extended beyond that required by the treaties.

The DMCA does not require on-line providers to adhere to its procedures, nor does it supercede or alter existing statutory or case law related to copyright. Any defense, which would otherwise be available to a provider, remains available.

Portions of the following document are taken verbatim and/or summarized from the text of the DMCA or other sections of the body of copyright law. Individuals interested in copyright law are strongly encouraged to review the sources listed and Title 17 U.S.C §512 especially.

DMCA Provisions for Online Service Providers

Limiting Liability - Under the DMCA, Online Service Providers can limit their liability for the copyright infringement of their users under certain circumstances as listed in Title 17 U.S.C. §512:

- Intermediate and/or transient storage of materials in the course of transmitting, routing, or providing connections
- System Caching
- Placing information on a system or network at the direction of users
- Use of information location tools, such as directories, indexes and hypertext links

Qualifications - In order for an OSP to qualify for the limitations on their liability, they must:

1. Register an agent with the U.S. Copyright office designated to received notifications of claimed infringement
2. Not have direct knowledge of infringing behavior
3. Not receive a financial benefit directly tied to the infringing activity
4. Provide to all users of its system or network information that accurately describes and promotes compliance with the laws relating to copyright
5. Provide and promote a policy of termination of service to individuals that are repeated infringers of copyright
6. Accommodate and not interfere with "standard technical measures" employed by copyright owners to identify and protect copyrighted works

7. Make reasonable attempts to request a properly formatted notification of a claimed infringement upon the receipt of an notification that does not substantially include the list below

8. Act expeditiously to remove or disable access to infringing material upon notification of a claimed infringement

9. Notify the user of the infringement claim and "takedown" action. Optionally inform the user of their right to issue a counter-notification

10. Notify the complaining party of the action taken

11. Upon receipt of a counter-notification, notify the original complaining party of the counter-notification

12. Repost or re-enable access to the work in question upon receipt of a counter-notification in no less then 10 days and no more than 14 days, unless they receive notice of intent to pursue legal action from the complaining party

**Notification** - To qualify as a properly formatted notification of a claimed infringement, such notification must substantially include:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

- Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

- Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

- A statement that the complaining party has a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

- A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

**Counter-Notification** - To qualify as a properly formatted counter-notification, an alleged infringer must include:
A physical or electronic signature of the subscriber

Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled

A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled

The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located [...] and that the subscriber will accept service of process from the person who provided notification [...] or an agent of such a person

The DMCA has further provisions directly related to nonprofit educational institutions. The actions of a faculty member or graduate student will not be construed as actions of the institution *unless* the infringing activity involves a faculty member or graduate student accessing instructional material that have been recommended or required for a course taught by the individual at the institution within the previous three years. There is also a provision removing the limitation of liability if the institution has received more than two properly formatted notifications of infringement within the previous three years for a specific faculty member or graduate student.

**Recommendations**

The DMCA liability limitation provisions place a significant amount of the workload on the OSP. Additionally, it is noteworthy that there is no provision for due process in the steps listed above. While the burden remains on ASC with these recommendations, they are intended to ensure the rights of the individual.

**Process**

**Copyright agent** - ASC should immediately register an agent with the copyright office to handle all claims of copyright infringement. The choice of the agent must be carefully considered:

"Campus-designated agents will be called on to make sensitive decisions that, if not exercised with care and good judgement, could impinge on academic freedom. It is essential that agents be appropriately positioned to determine whether to seek academic policy or legal advice as needed before taking administrative action. Agents should have ready access to information systems administrators, counsel, and representatives of the academic administration and the Academic Senate."

**Listing of Information** - The contact information should be listed on a newly developed and well-advertised webpage discussing copyright law, including provisions for termination of service to individuals that are repeat infringers. The guidelines established in Title 17 USC §512e suggest a termination of access if the user has more than two infringements (not alleged infringements) in a three year period.
Additionally, ASC should seek legal council clarifying our rights and protections under "common carrier" status as well as clarification regarding attribution of actions by undergraduate students to the institution.

**Receiving Notification of Claimed Infringement:**

1. Upon receiving a notification of claimed infringement, *regardless of whether it is properly formatted*, the designated agent should identify the alleged infringer and determine the circumstances of the alleged infringement.

2. Should a notification not be properly formed, the designated agent should make multiple attempts to secure the additional information to allow ASC to fall back on the DMCA liability clauses, should that be the best course of action for the specific infringement claim.

3. Based on the circumstances of the alleged infringement, a determination should be made whether the infringement falls under "fair use".

4. Should the alleged infringement fall under "fair use", the alleged infringer should file a counter-notice.

5. If the infringement does not fall under "fair use" the designated agent should request that infringing materials be taken down by the infringer.

6. If deemed necessary, hold internal judicial proceedings to determine the *fact* of infringement

7. Notify the complaining party of the action taken.

**Receiving a Subpoena for Information**

While subpoena's filed under the provisions of the DMCA do not require judicial review, we should honor them to the fullest of our abilities using the existing internal mechanisms for responding to subpoenas.

**Further Notes**

**Seeking Protection** - The practice of choosing, case by case, whether to seek protection under Title 17 USC §512 appears to be the course of action chosen by the University of Florida, the University of California, and the University of Texas System. Actions taken should be based on substantiated fact, not solely upon allegation. The technical measures mentioned in qualification point 6 above are, as yet, undefined. There is potential that the rate-limiting effects of using packet shaping on outbound traffic could be construed as interfering with copyright holder's abilities to identify infringing materials, thus removing our rights to seek shelter under the provisions of the DMCA.

**Sovereign Immunity** - While ASC should exercise due diligence in ensuring proper administrative use of copyrighted materials, we have the ability to claim sovereign immunity in any possible copyright lawsuit that we may face. This should only be considered as a last defense
as there is currently a bill in the House of Representatives (HR2344)\textsuperscript{10} that would require states to forgo their rights to sovereign immunity in order to enforce their own copyrights.

Recently, there has been some concerns\textsuperscript{16} regarding copyright holders going after the alleged infringer directly without first providing the OSP with notice. They don't have to:

\textit{The 'notice and takedown' process provides a new, low-cost method of dealing with online infringement, but its use by copyright holders is not mandatory}\textsuperscript{2}.

\textbf{Definitions}

\begin{itemize}
  \item Berne Convention - properly known as the Paris Act of July 24, 1971 of the Berne Convention for the Protection of Literary and Artistic Works.
  \item DMCA - The Digital Millennium Copyright Act augments the existing copyright law espoused in Title 17 USC.
  \item WIPO - The World Intellectual Property Organization is a subcommittee of the United Nations
  \item OSP (Online Service Provider) - An entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received\textsuperscript{4}.
  \item Fair Use - The fair use of a copyrighted work including such use by reproduction in copies or phono-records or by any other means specified by that section [Title 17 USC §106], for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include –

    1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
    2. the nature of the copyrighted work;
    3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
    4. the effect of the use upon the potential market for or value of the copyrighted work\textsuperscript{14}
  \item Copyright Infringement as opposed to theft - It follows that interference with copyright does not easily equate with theft, conversion or fraud. The Copyright Act even employs a separate term of art to define one who misappropriates a copyright: 'Anyone who violates any of the exclusive rights of the copyright owner,' that is, anyone who trespasses into his exclusive domain by using or authorizing the use of the copyrighted work in on of the five ways set forth in the statute, 'is an infringer of the copyright.' -- US Supreme Court Justice Harry Blackmun\textsuperscript{11}
\end{itemize}
Resources