Acceptable Use
Policy# 01.A – 01.A.7
Approved: 03/01/04

01.A. 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.C, pg. 8), 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:

Authority

This policy was reviewed and approved by the Cabinet on March 01, 2004.

01.A.1. Usage Guidelines

01.A.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.A.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.A.1.c. Storage/Bandwidth - 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.A.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.A.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.A.3. **Account Access**

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

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

01.A.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.A.3.e. **Transferring authorization** - The privilege of using ASC equipment, wiring, computers 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.A.4. **Proper Use of Computing Resources**

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

01.A.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.A.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 are expressly forbidden.

01.A.4.e. **File Storage** - Network resources have been allocated and installed to ensure 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.A.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.A.5. **Use of Licensed Software and Copyrighted Electronic Materials**

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

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

01.A.6. **Privacy Considerations**

01.A.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.A.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.A.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.A.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.A.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.
Account Use  
Policy 01.B – 01.B.4  
Approved: 03/01/04

01.B. Purpose

This policy outlines the responsibilities of those creating, managing, and using college computer system accounts.

Authority

This policy was reviewed and approved by the Cabinet on March 01, 2004.

01.B.1. General

01.B.1.a. Central Management - Computer accounts for access to major college computer resources are managed and administered centrally by Computing Services (CS).

01.B.1.b. For College Business - Computer accounts are granted to ASC faculty, staff, and students for bona fide purposes related to their work or studies at the college. *State of Colorado Fiscal Rule* prohibits the use of State equipment or resources for private purposes. Therefore, use of college computer accounts, computer and communications equipment, software, and networks for commercial purposes is strictly prohibited. Incidental personal usage not related to college business is permitted, provided it does not materially interfere with the availability of services for college purposes.

01.B.1.c. Not to be Shared - Generally, only one person is authorized to use any particular account, although some individuals may own more than one account. The account owner is responsible for all use of the account. Each person should use only those computer accounts that have been created for his/her use. The negligence of another user in revealing an account name and password is not considered authorization for use. Account owners should make appropriate use of the system protection features. Items such as regularly changing of password(s) and maintaining confidentiality of password(s) would constitute as a good use of system protection. Account owners should also take precautions against others obtaining access to their computer resources such as an unattended, non-password protected desktop computer. Computer accounts should not be shared.

01.B.1.d. Office email accounts - In some instances, office email accounts will be authorized by and assigned to a particular department head or assignee. This person is responsible for all use of the account, and for notifying CS when the account is no longer needed.
01.B.1.e. **Password Security** – Passwords are the primary security mechanism protecting the contents of a computer account. Account owners are responsible for maintaining the passwords for their accounts. Passwords for administrative computer accounts should be changed every thirty days. Compliance is the responsibility of the account owner. Account owners should avoid choosing passwords that might be easily guessed by others. CS may require account owners to change their password, if there is reason to believe that a particular password has been, or may easily be, compromised. Lost (forgotten) passwords are reset only upon verification of identity.

01.B.1.f. **Revoking accounts** - CS may revoke access at any time if computing privileges are abused, or in the course of CS troubleshooting it is discovered that system problems are being caused by that account. Individuals should refer to the ASC Acceptable Use Policy (Policy #01.A; pg 1) for more information.

01.B.1.g. **Email forwarding** - Accounts with email access have the ability to forward all messages to another email address. When an account is deleted, any existing email forwarding is removed. In the case of a legal name change the old email account can be forwarded to the new account for up to a 2-month period.

01.B.2. **Employee Accounts**

01.B.2.a. **Creation** - Employee accounts are created after all required payroll information has been entered into Banner and following receipt of a completed Account Request Form (Appendix E, pg 75).

01.B.2.b. **Requests** - College employees requesting accounts will be asked to complete an Account Request Form (Appendix E, pg 75). The form requires a signature of the employee as well as their supervisor or department head. The employee’s signature indicates that the requestor agrees to comply with the Acceptable Use Policy (Policy # 01.A; pg 1). Account owners are responsible for compliance with the Family Educational Rights and Privacy Act of 1974, and all policies of the college related to the use of the account.

01.B.2.c. **Deletion** – Accounts for faculty will be deleted when the faculty member no longer works for the college, as reported by the Office of Human Resources.

01.B.2.c.1. Accounts for non-faculty staff will be deleted when the staff member no longer works for the college, as reported by the Office of Human Resources.

01.B.3. **Student Accounts**

01.B.3.a. **Creation** - New student accounts will be activated at the beginning of every semester and throughout the semester.

01.B.3.b. **Access** - Students are automatically assigned accounts that provide access to email, the college network and modem pool, and the college’s “open” computer
labs. Use of the account signifies acceptance of the Acceptable Use Policy (Policy #01.A; pg 1) specifying the conditions under which the account is granted.

01.B.3.c. **Deactivation** – All student account are deleted every August.

01.B.3.d. **Withdrawals** - Any student who processes a complete withdrawal will have their account deactivated upon receipt of the withdrawal paperwork from the Student Affairs office.

01.B.4. **Special Purpose Accounts**

01.B.4.a. **Temporary accounts for Authorized Volunteers** - Under certain circumstances, individuals not affiliated with the college as employees or contractors may be considered "Authorized Volunteers," and be eligible for an account during the period of this volunteer service. This group might include certain retired employees (whether faculty or staff), fund raisers, or those working on specific projects for the benefit of the college. An Authorized Volunteer Account Request Form (Appendix F, pg 78) would be required from the responsible Provost/Vice-President that will indicate time-period that the account is needed and what access-rights are needed.

01.B.4.b. **Student worker accounts (aka workstudies)** – Workstudy accounts will be created at the request of the supervisor. The account(s) will expire at the end of each term. Expired or soon-to-be-expired accounts will be reactivated/continued upon the written request of the supervisor.

01.B.4.c. **Non-employee accounts** - Under certain circumstances a contract or agreement with the college may entitle an individual to a computer account. This type of account will be created and/or activated based on the request of the college representative. The account will be limited in functionality to only the capabilities required to complete the contract or agreement. The account will have an expiration date of no longer then one-year from the creation date. The expiration date can be changed at the request of the college representative.

01.B.4.d. **Non-registered students** - Non-registered students who participate in special programs and who pay a technology fee (which may be included in the program fee) will receive an account with a start and end dates as appropriate to the program.

**FORMS:**
Account Request Form (Appendix E, pg 75)
Authorized Volunteers Account Request Form (Appendix F, pg 78)
Electronic Communications
Policy #01.C – 01.C.7
Approved: 03/01/04

01.C.  Purpose

ASC permits its employees and students to use college-owned or operated electronic communication facilities for official college business. The college will not monitor or disclose the content of employees or student’s electronic communications except as otherwise provided in part 01.C.4.b (page 11) of this policy.

Authority

This policy was reviewed and approved by the Cabinet on March 01, 2004.

01.C.1.  Permissible Uses

Except as expressly permitted in part 01.C.2.a (page 8) of this policy, college-owned or operated electronic communication facilities are intended and shall be used solely for official college business including employee and student academic pursuits.

01.C.2.  Prohibited Uses

01.C.2.a.  Personal and Commercial Purposes - college-owned or operated electronic communication facilities shall not be used for personal or commercial purposes. However, occasional use of email, the Internet, and the WWW for personal purposes is permitted if it does not entail a direct cost to the college.

01.C.2.a.1.  The college reserves the right to place additional restrictions on the personal use of its electronic communication facilities if necessary or convenient to conserve network resources for official college purposes.

01.C.2.b.  Use by Other Persons - Only employees and students may use the college’s electronic communication facilities to initiate or receive electronic communications. The college may also authorize guests to use its electronic communication facilities. The VP of Finance & Administration must authorize “guest” use in writing.

01.C.2.c.  Other Prohibited Uses - college electronic communications facilities shall not be used to:
01.C.2.c.1. **Breach security** – Breach or attempt to breach the security of any electronic communications facility (including the unauthorized or intentionally deceptive use of network privileges, accounts, access codes, identifiers or passwords); access or use any electronic communication facility without authorization; or knowingly intercept, access, disclose, disrupt, damage, or destroy any electronic communication, or any data, software, or hardware without authorization.

01.C.2.c.2. **Spam** - Intentionally disrupt or interfere with others use of any electronic communication facility (e.g., spamming and mail bombs).

01.C.2.c.3. **Confidential Info** - Send or store confidential information without authorization.

01.C.2.c.4. **Copyrights** - Infringe copyrights or violate other intellectual property rights and laws.

01.C.2.c.5. **Harass** - Threaten, intimidate, harass, or defame others in violation of college policies or state and federal laws.

01.C.2.c.6. **Other** - Violate any other college policies or state and federal laws now or hereafter adopted.

01.C.3. **E-mail: Privacy; Ethics; Threatening, Intimidating, or Harassing Email**

01.C.3.a. **Privacy** - Current email technology does not guarantee privacy. Email is not like a telephone call or a letter in an envelope. The computer networks, over which it is transmitted, may be backed up and stored for long periods, automatically record information about email, including the sender and recipient’s names and addresses, the date, and the content of the communication. Many people in addition to the sender and recipient may have authorized or unauthorized access to some or all of this information. For example, if email is improperly addressed or there are problems with routing equipment, a postmaster may read the email to try to redirect it correctly. Similarly, breaches of network security may result in unauthorized access to or disclosure of email.

01.C.3.b. **Compromised privacy** - Email may be delivered to the wrong address as a result of user error or equipment failure. A recipient or recipients may store or print email or forward it to others including widely read mailing lists and newsgroups. Deleting email does not erase the copies that have been made during transmission and network backups. Even after email has
been deleted from a server or PC drive, it can sometimes be undeleted using specialized software. Because privacy cannot be guaranteed, it is important to exercise good judgment in drafting and sending email. Do not use email to communicate information that would be embarrassing or damaging to you or others if it were received by the wrong person or made public. It is advised that email not be used to communicate confidential information. Be careful, courteous and professional in choosing what to say and how to say it.

01.C.3.b.1. These precautions are equally applicable to facsimile communications.

01.C.3.c. **Encryption** - Employees and students may encrypt electronic communications only if they furnish the encryption key or software to the college upon request if decryption is necessary to monitor or disclose a communication under part 01.C.4.b (page 11) of this policy. Any electronic communication that may be of public record that is within the meaning of the *Colorado Public Records Act* or otherwise subject to monitoring or disclosure under this part 01.C.4.b (page 11) of this policy must be stored in clear text.

01.C.3.d. **Ethics and Etiquette** - A comprehensive summary of email ethics and etiquette is beyond the scope of this policy. However, please observe the following guidelines:

01.C.3.d.1. **Conserve network resources** - Do not send who-are-you messages, general broadcasts, chain letters, or mass mail.

01.C.3.d.2. **Mailing Lists** - Use good judgment in subscribing to mailing lists. Many lists are accessible by other means that use fewer network resources (e.g., through Usenet gateways or WWW pages). When subscribing to a mailing list, keep the description of list server commands. Ensure that you know how to unsubscribe and do so when you leave the college. If possible, set the list server to no mail during vacations and other lengthy absences from the institution. Retrieve and keep the lists FAQ (Frequently Asked Questions) file and comply with its policies and procedures. When sending email to a list, be sure that you know the difference between sending mail to an individual subscriber and sending it to the entire list.

01.C.3.d.3. **Misaddressed email** – If you receive an email intended for a colleague, let the sender know of the error and employ your professional conduct in your handling/knowledge of the content of that email.
01.C.3.d.4. **Forwarding** - Don’t forward confidential or personal email to other individuals, mailing lists or newsgroups without the original senders express or implied consent.

01.C.3.d.5. **Forged Names** - Remember that email can be sent under forged names and addresses.

01.C.3.d.6. **Passwords** - Don’t disclose your password to anyone or allow anyone else to use your account.

01.C.3.d.7. **Flame** - Do your best to ignore flame bait and flame wars.

01.C.3.e. **Threatening, Intimidating, or Harassing, Communications** - Except for automatic scanning by network security software, the college does not screen email and other electronic communications received by employees and students and generally cannot control their content. However:

01.C.3.e.1. If you receive threatening, intimidating or harassing email or facsimile communications, report the matter to Public Safety. Under some circumstances, the communications may violate the law and/or this and other policies.

01.C.4. **Monitoring and Disclosure of Content**

01.C.4.a. **In General** - The College will not routinely monitor or disclose the content of electronic communications sent, received, or stored using college-owned or operated electronic communication facilities.

01.C.4.b. **Exceptions** - As the owner or operator of electronic communication facilities and a public institution of higher education subject to the *Colorado Public Records Act*, §§2472101 et seq., C.R.S. (as now and hereafter amended), the college may monitor or disclose the content of employees and students electronic communications under the following circumstances:

01.C.4.b.1. A party to the communication consents; or

01.C.4.b.2. The communication is readily accessible to the public (for example, a WWW page, email sent to a public mailing list, or a newsgroup post); or

01.C.4.b.3. Monitoring or disclosure of an electronic communication is in the normal course of college employees employment and is necessarily incident to the maintenance of the college’s
electronic communication facilities, the rendition of electronic communication services, or the protection of the college’s rights or property (examples include but are not limited to routine maintenance, troubleshooting, or investigating an excessive use of network resources that adversely affects performance); or

01.C.4.b.4. Monitoring or disclosure of an electronic communication is: (i) based on an individualized suspicion that an employee or student has violated this policy, other college or Trustee policies, or state or federal law; and (ii) limited in scope to an investigation of the suspected violation; or

01.C.4.b.5. The college is legally obligated to monitor or disclose an electronic communication.

01.C.4.b.5.1. The Colorado Public Records Act defines public records as any documentary materials, regardless of physical form or characteristics expressly including electronic mail messages, that are maintained or kept by the state or any ... institution ... thereof for use in the exercise of functions required or authorized by law or administrative rule or involving the expenditure of public funds, §2472202, C.R.S. Employees are cautioned that electronic communications sent, received, and/or stored using college-owned or operated electronic communication facilities may be public records subject to public inspection and disclosure under §2472203 of the Public Records Act!

01.C.4.b.5.2. Warrants, subpoenas, court orders and discovery requests submitted under the Federal or Colorado Rules of Civil Procedure may require the college to monitor or disclose electronic communications.

01.C.5. Retention and Archival Storage
01.C.5.a. **State and college records policies** - State laws and college record-keeping policies apply to records created or stored in digital format including electronic communications.

01.C.5.b. **Employees responsibilities** - are responsible for copying electronic communications for storage in departmental or office Files.

01.C.5.b.1. **Archives** - ASC does not maintain centralized or distributed archives of electronic communications sent or received over its electronic communication facilities. Backups made for maintenance or troubleshooting purposes are erased at regular intervals.

01.C.5.b.2. **Copies** - Individual employees are responsible for making and keeping copies of electronic communications sent or received by them if the communications appear to be:

01.C.5.b.2.1. Public records under the *Colorado Public Records Act*; and,

01.C.5.b.2.2. Appropriate for preservation either as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the college or because of the value of the official governmental data they contain.

01.C.5.b.3. **Storage** - Employees should periodically store such copies in departmental or office files for subsequent review followed by either archival storage or destruction in accordance with general college record-keeping policies and the *State Archives and Public Records Act*, §§2480101 et seq., C.R.S. However, email received by employees need not be retained for review and storage unless the recipient has previously segregated and stored such messages as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the value of the official governmental data contained therein. §2480101 (1) (f), C.R.S. (emphasis added).

01.C.5.c. **Copying, Storage, and Inspection**

01.C.5.c.1. **Short-term Electronic Storage** - Electronic communications may be copied and saved to a workstations hard drive or to floppy disks. However, because of rapidly evolving
technologies, deterioration of storage media, and the risk of deliberate or inadvertent alteration, long-term digital storage is discouraged.

01.C.5.c.2. **Long-term Storage** - Whenever practicable, electronic communications should be transferred to and stored in more durable formats such as printouts copied to acid-free paper, microform, or other technologies such as CD-ROM.

01.C.5.c.3. **Inspection and Copying of Electronic Records** - Public records that are kept in digital format shall be made available for public inspection and copying on floppy disks, online, and/or as printouts in accordance with §§2472203 (1) (b) & 205, C.R.S. To facilitate compliance with the *Public Records Acts* very short deadlines for producing public records for inspection and copying, employees, departments, and or offices shall store digital records using a database or other electronic filing system that permits prompt identification and retrieval of the requested records.

01.C.6. **Violations**

Violations of this policy may result in disciplinary action up to and including termination or expulsion in accordance with the *State Colleges in Colorado Handbook for Professional Personnel*, the *State Personnel Systems* rules and procedures, and college policies. In addition, the college reserves the right to delete any electronic communication that violates part 01.C.2 (page 8) of this policy from its electronic communication facilities.

01.C.7. **Relationship to other college “Computing/Network Facilities Use” policies**

This policy supplements and does not supersede other college policies governing the appropriate or acceptable use of computing and network facilities.
Definitions

- **Confidential** - means a restriction placed on access to information by federal or state laws (including administrative regulations), court orders and rules, contracts, licenses, or Trustee and college policies.

- **Content** - means any information concerning the substance, purport, or meaning of an electronic communication.

- **Direct cost** - means a cost, fee or charge that would not otherwise be incurred by the college (for example, long distance telephone charges and printing costs).

- **Electronic communication** - includes, but is not limited to electronic mail (email), newsgroup posts, World Wide Web (WWW) pages, data or file transfers, and facsimile communications sent, published, or received by employees or students using college-owned or operated electronic communication facilities. Electronic communication includes any electronic communication that has been stored on a college-owned or operated network server, workstation, or personal computer or on removable media such as floppy or zip disks and tape. It does not include ordinary telephone communications.

- **Electronic communication facilities** - includes, but is not limited to public, private, and commercial computer networks (including the Internet), and facsimile facilities.

- **Employees** - all full and part-time, temporary and regular college employees including faculty members, administrators, classified personnel, and student employees.

- **Monitor** - to intercept, access, or inspect an electronic communication. Monitor does not include automatic scanning of an electronic communication by network security software such as firewall and anti-virus programs.

- **Students** - students who are currently enrolled and in good standing at the college.
Login Names for -Faculty & Staff
Policy #01.D – 01.D.3
Approved: 03/01/04

01.D. Purpose

In order to maintain security ASC requires a login or registration to use the network. Computing Services (CS), in working towards creating a single login to the network, must put some restrictions on the structure of the login name due to system and administration constraints.

Authority

This policy was reviewed and approved by the Cabinet on March 01, 2004.

01.D.1. Structure rules - The following are the necessary rules for establishing a login-name that can work throughout the various computer systems.

- Max length: 32 characters
- Required: must include your last name, no spaces, all lower case
- Characters allowed: regular English alphabet, _, numbers
- Recommended: “preferred name” _ “last name”

Examples: bob_smith rf_smith
bobbysmith rfsmith
robertsmith smith24

- No profanity, no vulgarities, no sexual innuendos, or etc. will be allowed.

01.D.2. Disallowed - ASC reserves the right to disallow any login name.

01.D.3. Unique - All login names on campus must be unique, so if someone already has what you want for a login name, another login name will need to be selected.
Login Names for Students
Policy #01.E – 01.E.4
Approved: 03/01/04

01.E. Purpose

In order to maintain security ASC requires a login or registration to use the network. Some restrictions on the structure of the login name will need to be put in place due to system and administration constraints.

Authority

This policy was reviewed and approved by the Cabinet on March 01, 2004.

01.E.1. Structure rules - The following are the necessary rules for establishing a login-name that can work throughout the various computer systems.

- Max length: 32 characters
- Required: must include your last name, no spaces, all lower case
- Characters allowed: regular English alphabet, numbers
- To facilitate the computer generation of login names, the following rules will be used to generate these login names:
  - 1st choice: “last name”“FI”“MI”
    Possible required variation: “last name”“FI”“MI”[002]
  - Examples: “smithrf”
    “smithrf02” - if more than 1 “smithrf” exists

01.E.2. Disallowed - ASC reserves the right to disallow any login name.

01.E.3. Login name problems - If a generated login name results in a problem login name, CS will work with the student to create an acceptable login name.

01.E.4. Reused - Login names will not be reused for one-year after being deactivated.