

## ALVIN COMMUNITY COLLEGE COMPUTER AND TECHNOLOGY USE POLICY

### **PURPOSE**

Alvin Community College provides computer and Internet resources to its students, faculty, and staff as a means of enhancing learning, efficiency, and productivity. Commercial uses are specifically excluded. ***All students, faculty, and staff are responsible for seeing that these computing resources are used in an effective, efficient, ethical, and lawful manner.*** This policy establishes rules and prohibitions that define acceptable use of these computing systems. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as discipline or legal sanctions under Federal, State, and local law. Copies of these laws and/or policies are available at the Alvin Community College Library.

### **USERS AGREEMENT**

All users of Alvin Community College computing resources must read, understand, and comply with this policy, as well as any additional guidelines established by the administrators of each system. **By using any of these systems, users agree to comply with these policies. All users are required to acknowledge receipt and understanding of all College policies and administrative procedures governing use of the system and agree in writing to comply with such policies and procedures.**

### **RIGHTS**

These computer systems, facilities, and accounts are owned by and operated by Alvin Community College. The College reserves all rights, including termination of service without notice, to the computing resources which it owns and operates.

### **PRIVILEGES**

Access to the College's network system and the Internet is a privilege, not a right. Access and privileges on Alvin Community College computing systems are assigned and managed by the administrators of the specific systems. A system administrator is the person or persons appointed by the College administration to monitor computer resources in a selected area or areas. Eligible individuals may become authorized users of a system and be granted appropriated access and privileges by following the approval steps prescribed for that system.

All access to the College computer resources, including the issuance of passwords, must be approved by the Director of Information Technology.

## **CONFIDENTIALITY**

No user is to disclose confidential information unless disclosure is a normal requirement of that user's position and has been so authorized. All users with access to confidential data are to safeguard the accuracy, integrity, and confidentiality of that data by taking precautions and following procedures necessary to ensure that no unauthorized disclosure of confidential data occurs. Such precautions and procedures include the secure storage of data backups and the protection of sensitive data with passwords.

## **USAGE**

### **Accounts and Files**

All accounts, including email, are the property of Alvin Community College. As such, any information associated with these accounts is not private.

Accounts on any College-owned computer are limited to current employees and current students.

Access to College networks is restricted to Alvin Community College faculty, currently enrolled students, and staff. Community members and others who do not meet these requirements are allowed access at Alvin Community College's Library.

All authorized users are solely responsible for managing their files (including the files that constitute a web course) and their email.

Accounts may be deleted when employment is terminated, when student status has ended, or at the discretion of the Administration of the College and/or the discretion of the administrator of the network. The college is under no obligation to recover or protect user files from deleted accounts.

Users are to take precautions to prevent the unauthorized use of their passwords. In choosing passwords, users are to avoid the use of common words, proper names, readily associated nicknames or initials, and any other letter and/or number sequences that might be easily guessed. Users will be held accountable for all actions performed under their passwords, including those performed by individuals as a result of user negligence in protecting the codes. If passwords become compromised, users are to change them immediately or contact the Director of Information Technology at 281.756.3536.

Users are not to attempt to access, search, or copy technological and information resources without the proper authorization. No one is to use another individual's account without permission, and active sessions are not to be left unattended. Users are not to test or attempt to compromise internal controls, even for purposes of systems improvement. Such actions require the advance, written approval of the authorized administrator, or must be included among the security evaluation responsibilities of one's position. Violations must be reported to the Director of Information Technology.

## **COPYRIGHT ISSUES**

Copyright is a form of protection that the law provides to the authors of "original works of authorship" for their intellectual works that are "fixed in any tangible medium of expression", both published and unpublished (Title 17, United States Code). It is illegal to violate any of the rights provided by the law to the owner of the copyright. Alvin Community College respects the ownership of intellectual material governed by copyright laws. All users of Alvin Community College technology resources are to comply with the copyright laws and the provisions of the licensing agreements that apply to software; printed and electronic materials, including documentation, graphics, photographs, multimedia, including musical works, video productions, sound recordings, and dramatic works; and all other technological resources licensed and/or purchased by Alvin Community College or accessible over network resources provided by Alvin Community College.

In compliance with the requirements of the Digital Millennium Copyright Act of 1998 (DMCA), any user of Alvin Community College technology resources who violates the digital copyright laws for the first time will be reminded of the laws, and the software or licensing violation will be removed. A second violation will result in removing the software or licensing violations, retraining the user in copyright procedures, and taking appropriate disciplinary action. A third violation will require Alvin Community College to remove the user's network and Internet access and take further disciplinary action which may include termination of Alvin Community College employment or student status.

## **THE INTERNET**

Alvin Community College's Internet resources, including the World Wide Web, electronic mail, and file transfer protocol (FTP) provide information beyond the confines of the campus. It allows access to ideas, information, and commentary from around the world. While the Internet offers a wealth of material that is personally, culturally, and professionally enriching to individuals of all ages, it also enables access to some material that may be offensive or disturbing to others, inaccurate, or illegal under U.S. law. Alvin Community College can not police the global network and takes no responsibility for its content. Rather, all users must take responsibility for their own activities on the Internet.

The use of the Internet must be consistent with the mission of Alvin Community College, the policies of the College, State, and Federal law. Access to the Internet over college computers is a privilege granted to users, and the College reserves the right to suspend this privilege if a user violates any acceptable use clause.

## **EMAIL**

### **Account Activation/Termination**

Email is a critical mechanism for business communications at Alvin Community College. However, use of Alvin Community College's electronic mail system and services is a privilege, not a right; and therefore, must be used with respect and in accordance with the goals of Alvin Community College.

All employees of Alvin Community College are entitled to an email account. Email accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include auditors or contractors.

Applications for these temporary accounts must be submitted in writing to the Director of Information Technology. All terms, conditions, and restrictions governing email use must be in a written and signed agreement.

Email access will be terminated when the employee or third party terminates his or her association with the College, unless other arrangements have been made. Alvin Community College is under no obligation to store or forward the contents of individual's email inbox/outbox after the term of their employment has ceased.

### **General Expectations of End Users**

Important official communications are often delivered via email. As a result, employees of Alvin Community College with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important college announcements and updates, as well as fulfilling business- and role-oriented tasks.

Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove him or herself from the list, and is responsible for doing so in the event that their current email addresses changes.

Email users are also expected to comply with normal standards of professional and personal courtesy, and conduct.

## **VIRUSES**

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via email, instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Alvin Community College in terms of lost data and lost staff productivity.

Alvin Community College has anti-virus software licensed per individual computer. If a user receives what he/she believes to be a virus, or suspects that a computer is infected

with a virus, it must be reported to the IT Department at 281.756.3544. Report the following information if known: virus name, extent of infection, source of virus, and potential recipients of infected material.

**Rules for Virus Prevention**

1. Run the standard anti-virus software provided by the College. Contact IT at ext. 3544 for assistance.
2. Never open any files or macros from an unknown source.
3. Be suspicious of email messages containing links to unknown Web sites.
4. Never copy, download, or install files from unknown sources.
5. Regularly update virus protection on personally owned home computers that are used for business purposes.

**TELEPHONE AND VOICEMAIL ACCEPTABLE USE POLICY**

Telephone communication is an essential part of the day-to-day operations of Alvin Community College. Telephone and voicemail services are provided to employees of the College in order to facilitate performance of the College's work. At this time, due to costs, Adjunct Faculty do not have access to a voicemail box.

As with all Alvin Community College resources, the use of telephones and voicemail should be as cost effective as possible and in keeping with the best interests of the College. All employees must operate within the following basic policy guidelines:

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Alvin Community College.
- The Information Technology Department is responsible for installation and repair of all college telephony equipment and administration of telephone and voicemail accounts.
- If a voicemail box is full, no further messages can be recorded.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Use of directory assistance (i.e., 411) should be avoided since a fee is incurred with each use.
- Five business days' notice is required to set up a standard telephone service and voicemail box.

**WIRELESS SECURITY ACCESS**

Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Alvin Community College does not automatically guarantee the granting of wireless access privileges.

Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are used for general purpose access in areas of transient use, such as common areas or meeting

rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

Addition of new wireless access points within college facilities will be managed at the sole discretion of the Information Technology Department. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are strictly forbidden and may result in the seizure of that equipment.

An application process is required to be granted wireless access. Please contact the Network Manager at 281.756.3544 for an application.

### **INSTANT MESSAGING**

Instant Messaging (IM) is currently being used at Alvin Community College as a form of real-time chat communication with individuals both inside and outside the organization. While the use of IM is not banned, it currently is not supported by the Information Technology Department and carries some security risks that must be addressed.

IM use at the College is a privilege, and its abuse will not be tolerated. It is the user's responsibility to ensure that IM software is set to the highest security settings possible and is used responsibly.

#### **Common IM Packages**

The following four free IM services are the most commonly used by ACC employees:

- AOL Instant Messenger
- ICQ
- MSN Messenger Service
- Yahoo! Messenger

If college personnel are using an IM service other than the four listed above, please notify the Information Technology Department at 281.756.3544, as use of IM services could affect network security. The firewall may be configured to block effective functioning of the IM service of choice. No change will be made to the college's firewall to allow IM service unless it is specifically related to college business.

### **REMOTE ACCESS**

Remote access is defined as any connection to Alvin Community College's network and/or other applications from off-site locations, such as the employee's home, a hotel room, airports, cafes, satellite office, and wireless devices.

All remote access will be centrally managed by Alvin Community College's Information Technology Department and will utilize encryption and strong authentication measures. Remote access connections covered by this policy include (but are not limited to) Internet dial-up modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

All employees requiring the use of remote access for business purposes must go through an application process that clearly outlines why the access is required and level of service the employee needs. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the Information Technology Department. Please contact the Help Desk, ext. 3544 for an application.

## **BACKUPS**

It is the responsibility of the appropriate administrator or network administrator to ensure that appropriate procedures and resources are in place to back up data on a regular basis. Backups are to be stored in a location that is physically secure to protect the confidentiality of the data. It is the responsibility of the user to perform any actions necessary to comply with these procedures.

## **PHYSICAL SECURITY**

All users are responsible for the physical security of their technological and information resources. Administrators are to help ensure physical security by instituting procedures for the use of locked doors and/or for the use of security devices made available by Alvin Community College for the protection of the equipment. To avoid loss by fire or theft, backups of important data are not to be stored in the same location as the originals.

Adequate power regulators and surge suppressers are to be used.

## **GENERAL PROVISIONS**

The following actions (including but not limited to) will result in disciplinary action including but not limited to the suspension of computer privileges:

1. Damage or destruction of equipment, software, or data belonging to the College or to other users, including adding, altering, or deleting files on College workstations and/or servers.
2. Altering of system settings or Internet browser settings on College computers without express permission of an instructor or an authorized member of the IT Staff.
3. Reproduction of materials protected by copyright without permission of the copyright owner.
4. Violating software license agreements.
5. Violating or attempting to violate computer system or network integrity, including attempts to bypass network security functions, or to obtain restricted passwords for system administration.
6. Using College technological resources to harass others.
7. Utilizing the Internet and/or College equipment for unauthorized material/commercial gain or profit.
8. Using the Internet or any College technological resource for any activity prohibited by Federal, State or International Law.

9. Attempting to utilize computing resources for which you do not have access.
10. Sharing your personal password with others or using another person's password.
11. Impersonating another user via any form of electronic messaging.
12. The production of and/or intentional dissemination of self-replicating or similar nuisance program (e.g., virus, Trojan horse), whether or not they are destructive in nature.

## **MAINTENANCE**

The responsibility for maintaining the campus computing environment rests with the Department of Information Technology. In order to ensure the smooth functioning of computer equipment, all students, faculty, and staff must observe the following:

1. Only authorized software may be installed on any College computer. The IT Department is responsible for determining what software may or may not be installed, based on technical specifications and licensing.
2. Only authorized IT personnel may repair College computer equipment.
3. Maintenance requests for labs should be submitted in a timely fashion; i.e., at least two weeks in advance. A list of all required software and proof of licensing should be provided to the technician at that time.
4. Only college-owned equipment will be allowed onto Alvin Community College's network (exception: student wireless equipment).

## **VIOLATIONS**

A user's privileges may be suspended immediately upon the discovery of a possible violation of these policies. Suspected violations will be confidentially reported to the appropriate system administrator and employee's supervisor.

Violations of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College, and legal action. Violations of some of the above policies may constitute a criminal offense.

## Alvin Community College

### User Agreement of Understanding

Access and use of the Internet, email, authorized software, local area networks, computers, and other related equipment is a privilege for the user. Alvin Community College has developed a Computer and Technology Use Policy for the Internet, email, authorized software, local area networks, and other related equipment.

I have read the attached Alvin Community College Computer and Technology Use Policy for the Internet, authorized software, local area network, computers, and other related equipment. I hereby agree to be responsible for and abide by all rules and regulations of this policy.

---

User Signature

Date

---

User Printed Name

Please check all that apply:

- Employee
- Faculty
- Student