ALVIN COMMUNITY COLLEGE	ADMINISTRATIVE PROCEDURE MANUAL	
Section Title: Technology Use Standard and Agreement - Employee	Number: cr-05	Page: 1 of 12
BASED ON BOARD OF REGENTS POLICY		
Policy Title: TECHNOLOGY RESOURCES	Policy Number: CR	
Local	Date Adopted by ELT: 12/12/17	

Purpose

The purpose of this procedure is to provide guidance to employees on the acceptable use of the college technology resources.

1. Background

Alvin Community College provides computer and Internet resources to its employees as a means of enhancing efficiency and productivity. Commercial uses are specifically excluded. All employees are responsible for seeing that these computing resources are used in an effective, efficient, ethical, secure, and lawful manner. This standard 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.

2. Users Agreement

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

3. Rights and Privileges

The 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.

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.

Limited personal use of the college's technology resources are permitted if the use:

1) Imposes no tangible cost to the college;
2) Does not unduly burden the college's technology resources; and
3) Has no adverse effect on an employee's job performance or a student's academic performance.

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

4. 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.

5. Usage

a. 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.

Access to College networks is restricted to Alvin Community College faculty, currently enrolled students, staff, and trusted vendor partners. Community members and others who do not meet these requirements are allowed access within Alvin Community College's Library, or through the College's guest Wi-Fi.

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

Accounts are marked for deletion when employment is terminated 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 a user's personal 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. Passwords should contain a mix of upper case, lower case and numeric characters and special characters. 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 password. If an account becomes compromised, users are to immediately change their password and contact the IT Service Desk.

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, 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 and 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, employee's supervisor, and Office of Human Resources.

b. Elevated Access and Permissions

Users with access to student and personnel systems are not to modify or add approvals to their own records. Users whose primary role is to modify such records must notify their supervisor should any such change be necessary to their record, and are expected to follow standard college approval procedures.

Users with elevated permissions or administrative access should only use those accounts for official college business. Use of administrative access should be consistent with an individual's role or job responsibilities as assigned by the administrative tasks assigned to their job descriptions. Administrative access or elevated permissions must not be used to satisfy personal curiosity about an individual, system, practice, department, or other type of entity.

6. 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.

7. The Internet

Alvin Community College's Internet resources, including the World Wide Web, electronic mail, and networking protocols 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 academically, personally, culturally, and professionally enriching to individuals of all ages, it also enables access to material that may be offensive or disturbing to others, inaccurate, or illegal under U.S. law. Alvin Community College cannot 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 and control this privilege if a user violates any acceptable use clause.

8. Email

a. Account Activation/Termination

Email is a critical mechanism for business communications at Alvin Community College. All employees are assigned an Alvin Community College email address to use throughout their employment. This Alvin Community College email address is the official means of communication within the 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.

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.

Employee 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 or has ceased.

b. Email Content

Employees should NOT include any personally identifiable information (PII) in an email message body or in an unencrypted attachment.

Examples of PII include *but not limited to* the following:

- Social Security Numbers
- Bank Account Numbers
- Health Status or information
- Credit Card numbers
- Driver's license number
- Mothers Maiden Name
- Birthdate
- Employment date or retirement eligibility date
- Race, ethnic, religion, or sexual orientation
- Home address and telephone number

c. 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.

9. Social Media Standards and Guidelines

Social media has changed the way we communicate, offering a new model to engage with students, alumni, and the world at large. The Alvin Community College Marketing department has created a dynamic set of standards and guidelines that will be adjusted as new mediums, issues, and practices in conjunction with the overall communication goals of the college arise.

By participating on social media profiles and websites officially administered by Alvin Community College, it is understood that user-generated content on college social media profiles or websites does not reflect the opinion or interests of ACC or its offices and must not be inappropriate in nature. All participation and user-generated content appearing on ACC's social media profiles is subject to this agreement

All participants on ACC social media profiles and websites must act appropriately and respectfully with the other participants in our online community. We ask that all participants in ACC's social media provides refrain from derogatory content which includes but is not limited to: Content which is illegal, blatantly profane, violent, sexual, pornographic, discriminatory, or otherwise defamatory. All content deemed inappropriate will be removed at the discretion of ACC Marketing and Communications administrators.

All content posted on pages and websites administered by ACC is subject to applicable copyright laws. User may only post content of which they are the owner(s) or have written or licensed permission from the copyright owner to share the content (i.e. under an attribution Creative Commons license).

ACC accepts no responsibility or liability for any data, text, software, images, videos, messages, audio, or other content, which is generated by and posted publicly by users other than ACC in its official capacity. ACC accepts no liability or responsibility whatsoever for the content of any target third-party site linked from this page.

The entirety of Alvin Community College's Social Media Standards and Guidelines is available through the Marketing and Communications department, and must be reviewed and accepted prior to engaging in any social media activity which may be construed as being on behalf of the college.

10. Protecting College Data

Alvin Community College Information Technology utilizes a number of networked devices and strategies to protect college data from cyber related attacks. However, it is every employee's responsibility to safeguard their network credentials and college data. Employees should be alert to various attempts and strategies that may inadvertently allow malicious attempts to gain access to data. Any suspicious email or computer activity should be immediately reported to the IT Service Desk. College employees must participate in the Cyber Safety Awareness Training and Testing Program. Users that fail to safeguard their network credentials or college data may face disciplinary measures, including the removal of all network privileges.

a. 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, and removable media, including mobile devices. 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 immediately to the IT Service Desk. Report the following information if known: virus name, extent of infection, source of virus, and potential recipients of infected material.

b. Rules for Virus Protections

1. Run the standard anti-virus software provided by the College. Contact the IT Service Desk immediately 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.

c. Phishing, SMishing, and Vishing

Phishing email messages and websites are designed to steal money or obtain access to data. Phishing attempts most often mimic an official looking email or website, and request the user's ID and password. Once a user fails to recognize the attempt and provide this information, cybercriminals can install malicious software on your computer or steal or encrypt and hold for ransom personal and college information off of your computer and networked drives.

Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. SMishing is a similar attempt using texting/SMS applications. Vishing is an attempt to gain access to your information over the phone.

i. Tips for Recognizing Phishing Attempts

- Don't trust the display name of the sender of an email. Check the email address in the header form – if it looks suspicious, don't open the email.
- Look but don't click – hover you mouse over any links embedded in the body of the email. If the link address looks suspicious, don't click on it.
- Check for spelling mistakes – These are often a good sign that the email is not legitimate.
- Beware of urgent or threatening language in the subject line – Invoking a sense of urgency is a common phishing tactic. Beware of phrases such as "account will be suspended", or "mailbox is at the limit".
- Never give out personal information – legitimate companies will never ask for personal credentials via email.

- Don’t believe everything you see - Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it’s legitimate. Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don’t open it.

11. Laptops, Tablets, and Mobile Devices

If issued a college laptop, or using a mobile device to conduct college business, employees must take adequate care to protect and secure it. Be aware of your surroundings and any suspicious persons. The device should never be left in an unsecured area in an automobile, hotel, or conference event. If circumstances require storing in a vehicle, the device must be kept in the trunk or completely out of sight. Employees that are assigned college-owned devices are solely responsible for their care. The college requires a copy of a police report should the assigned equipment be stolen or an insurance claim if damaged in a vehicular accident or natural disaster. College data should never be stored on a mobile device; secured remote access should be utilized to securely access college networked data.

12. Telephone and Voicemail Acceptable Use Standards

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. Adjunct Faculty are not assigned 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 standard guidelines:

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Alvin Community College.
- Information Technology Services 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.

13. Wireless 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 Information Technology Services in conjunction with key functional and instructional areas of the College. 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.

14. 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. 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.

15. 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, conference, airports, cafes, satellite office, and wireless devices.

All remote access will be centrally managed by Alvin Community College Information Technology Services and will utilize encryption and strong authentication measures.

Based on positions within the college, certain employees are automatically granted remote access privileges. Any other employee requiring the use of remote access for business purposes must request access through their supervisor and clearly outline why the access is required and level of service needed. Requests must be approved by the employee's dean, director, or vice president before submission to Information Technology Services. Please contact the IT Service Desk for more information.

16. 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.

It is important to note that only networked drives are included in the normal backup processes. Data stored on users' desktops or local hard drives are not backed up, and may not be recoverable in the event of a system failure. All college data must be stored in the user's personal network share or departmental drive.

17. 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.

18. 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:

a. 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.
b. Altering of system settings or Internet browser settings on College computers without express permission of an instructor or an authorized member of Information Technology Services.
c. Reproduction of materials protected by copyright without permission of the copyright owner.
d. Violating software license agreements.
e. 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.
f. Using College technological resources to harass or intentionally offend others.
g. Utilizing the Internet and/or College equipment for unauthorized material/commercial gain or profit.
h. Using the Internet or any College technological resource for any activity prohibited by Federal, State or International Law.
i. Attempting to utilize computing resources to which you do not have access or approval.
j. Sharing your personal password with others or using another person's password.
k. Neglecting to protect and safeguard network IDs and passwords, including phishing attempts and other cybercriminal methods.
l. Impersonating another user via any form of electronic messaging.

1. 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.

19. Maintenance

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

1. Only authorized software may be installed on any College computer. The Information Technology Services is responsible for determining what software may or may not be installed, based on technical specifications and licensing.
2. Only authorized ITS 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 may be requested by ITS before any work is performed.

20. Violations

An employee's computer use privileges may be suspended immediately upon the discovery of a possible violation of this Standard. Suspected violations will be confidentially reported to the appropriate system administrator, employee's supervisor, and Office of Human Resources.

Violations of this Standard 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, termination from the College, and legal action. Violations of some of the above standards may constitute a criminal offense.

Alvin Community College

User Agreement of Understanding - Employee

Access and use of the Internet, email, authorized software, local area networks, computers, and other related equipment is a privilege for the user. As defined in ACC Board Local Policy CR – Technology Resources, and DH – Employee Standards of Conduct, Alvin Community College has developed a Technology Use Standard for the internet, email, authorized software, local area networks, and other related equipment. All employees must review and sign this agreement upon hire and with each academic year.

I have read the attached Alvin Community College Technology Use Standard and Agreement. I hereby agree to be responsible for and abide by all rules and regulations of this Standard.

User Signature Date

User Printed Name