ALVIN COLLEGE	ADMINISTRATIVE PROCEDURE MANUAL	
Section Title: **Acceptable Use of Technology - Student**	Number: cr-06	Page: 1 of 7
BASED ON BOARD OF REGENTS POLICY		
Policy Title: TECHNOLOGY RESOURCES	Policy Number: CR	
Local	Date Adopted: 12/12/2017 Last Updated: 08/25/2026	

PURPOSE

The purpose of this procedure is to provide guidance to students on the acceptable use of Alvin College's technology resources.

BACKGROUND

Alvin College provides computer and Internet resources to its students as a means of enhancing learning, efficiency, and productivity. Commercial uses are specifically excluded. All students are responsible for using computing resources 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.

USERS AGREEMENT

All users of Alvin 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.

RIGHTS and PRIVILEGES

The computer systems, facilities, and accounts are owned by and operated by Alvin 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 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 appropriate access and privileges by following the approval steps prescribed for that system.

Student education records, including records maintained on Alvin College's information systems, are protected under the Family Educational Rights and Privacy Act (FERPA), in addition to any applicable public information laws.

MULTI-FACTOR AUTHENTICATION

"Multi-Factor Authentication (MFA)" is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism, typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
Alvin College students are required to register a device or alternative contact to provide a secure method for systems to contact you during the login process for email and other College systems. Depending on the MFA type and supported application, the device or alternative contact type may be a mobile device that can receive texts, an authentication app on a mobile device, a non-College email address, or a land-line telephone. The recommended and most secure method is an authentication app installed on a personal mobile device.

Dual enrollment students may be excused from mobile device-based MFA methods while on a high school campus, consistent with state law restricting student cell phone use during the school day. Affected students should use an alternative MFA method, such as a non-College email address or a land-line telephone, and may contact the IT Service Desk for assistance.

USAGE

Accounts and Files

All accounts, including email, are the property of Alvin College. As such, any information associated with these accounts is not private, unless specifically protected by privacy laws. Student users should store files on their College-provided cloud storage account.
Accounts on any College-owned computer are limited to current students.
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 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. Passwords should contain a mix of upper case, lower case, 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 the perceived purposes of systems improvement.

EMAIL

Email is a critical mechanism for academic communications at Alvin College. All students are assigned an Alvin College email address to use throughout their enrollment with the College. This Alvin College email address is the official means of communication within the College and its students. Use of Alvin 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 College.

Email Account Activation / Termination

Student email access will be disabled following one year of non-enrollment activity, whether due to graduation, certificate completion, transfer, or not returning to Alvin College. The student email account will be deleted following one year and one full semester of inactivity as described above.

General Expectations of End Users

Important official communications are often delivered via email. As a result, students of Alvin 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.

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 address changes.

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

Email Content – Do NOT include PII

Students should NOT include any personally identifiable information (PII) in an email message body or in an unencrypted attachment. Examples of PII include but are not limited to the following:

- Social Security Numbers
- Bank Account Numbers
- Health Status or information
- Credit Card numbers
- Driver's license number
- Mother's Maiden Name
- Birthdate
- Race, ethnicity, religion, or sexual orientation
- Home address and telephone number

THE INTERNET

Alvin 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 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 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 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.

COPYRIGHT CONCERNS

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 College respects the ownership of intellectual material governed by copyright laws. All users of Alvin 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 College or accessible over network resources provided by Alvin College.
In compliance with the requirements of the Digital Millennium Copyright Act of 1998 (DMCA), any user of Alvin 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 violation, retraining the user in copyright procedures, and taking appropriate disciplinary action. A third violation will require Alvin College to remove the user's network and Internet access and take further disciplinary action which may include termination of Alvin College student status.

AI AND MACHINE LEARNING

Artificial Intelligence (AI) and Machine Learning (ML) are technologies that allow computer systems to perform tasks that normally require human judgment, such as analyzing data, generating text or images, and supporting decision-making. AI and ML can enhance learning and coursework, but student use must be consistent with CRB-02, Acceptable Use of Artificial Intelligence, Student, this procedure, and applicable law.

SOCIAL MEDIA STANDARDS and GUIDELINES

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

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

All content posted on pages and websites administered by Alvin College is subject to applicable copyright laws. Users 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).
Alvin College 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 Alvin College in its official capacity. Alvin College accepts no liability or responsibility whatsoever for the content of any target third-party site linked from this page.
Artificial intelligence tools used to generate, edit, or plan content posted on Alvin College social media accounts must comply with CRB-02, Acceptable Use of Artificial Intelligence, Student, and the standards and guidelines outlined above.

WI-FI ACCESS

Wireless access to enterprise network resources is a privilege, not a right. Consequently, student enrollment at Alvin College does not automatically guarantee the granting of wireless access privileges. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the campus, are strictly forbidden and may result in the seizure of that equipment.

INSTANT MESSAGING

Instant Messaging (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.

REMOTE ACCESS

Remote access to the internal Alvin College network is not provided to students. Please contact the IT Service Desk for more information.

PROTECTING COLLEGE DATA

Alvin College Information Technology utilizes a number of networked devices and strategies to protect College data from attacks to gain access to it. However, it is every student's responsibility to safeguard their network credentials and College data. Students 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.

Viruses and Malware

Malware, traditionally known as a 'computer virus', is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Malware may be transmitted via email, instant messaging attachments, downloadable Internet files, and removable media, including mobile devices. Malware is usually disguised as something else, and so its presence is not always obvious to the computer user. A malware infection can be very costly to Alvin College in terms of lost data and lost productivity. Alvin College has anti-malware software licensed per individual computer. If a user receives what he/she believes to be malware, or suspects that a computer is infected, it must be reported to the IT Service Desk. Report the following information if known: name of the suspected malware, extent of infection, source, and potential recipients of infected material.

Rules for Malware Prevention

- Regularly update virus protection on personally owned laptops and home computers.
- Never open any files or macros from an unknown source.
- Be suspicious of email messages containing links to unknown Web sites.
- Never copy, download, or install files from unknown sources.

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 provides this information, cybercriminals can install malicious software on a computer, or steal or encrypt and hold for ransom personal and College information.

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

Tips for Recognizing Phishing Attempts

- Don't trust the display name of the sender of an email. Check the email address in the header; if it looks suspicious, don't open the email.
- Look but don't click; hover your 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 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; watch for 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; a convincing brand logo, language, or seemingly valid email address does not mean a message is legitimate. Be skeptical, and don't open anything that looks even remotely suspicious.

PHYSICAL SECURITY

All students are responsible for the physical security of their technological and information resources. To avoid loss by fire or theft, backups of important data are not to be stored in the same location as the originals.

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:

- 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.
- 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.
- Reproduction of materials protected by copyright without permission of the copyright owner.
- Violating software license agreements.
- 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.
- Using College technological resources to harass or intentionally offend others.
- Utilizing the Internet and/or College equipment for unauthorized material, commercial gain, or profit.
- Using the Internet or any College technological resource for any activity prohibited by Federal, State, or International Law.
- Attempting to utilize computing resources to which you do not have access or approval.
- Sharing your personal password with others or using another person's password.
- Neglecting to protect and safeguard network IDs and passwords, including phishing attempts and other cybercriminal methods.
- Impersonating another user via any form of electronic messaging.
- The production of and/or intentional dissemination of a self-replicating or similar nuisance program (e.g., virus, Trojan horse), whether or not it is destructive in nature.

MAINTENANCE

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

- Only authorized software may be installed on any College computer. Information Technology Services is responsible for determining what software may or may not be installed, based on technical specifications and licensing.
- Only authorized personnel may repair College computer equipment.

- 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 Information Technology Services before any work is performed.

LEGAL AND REGULATORY REFERENCES

This procedure is governed by, at minimum:

- Texas Government Code Chapter 2054, Subchapter S (Senate Bill 1964), which requires an AI Code of Ethics and minimum risk-management standards for AI systems;
- 1 Texas Administrative Code Chapter 219, which implements Senate Bill 1964, including the AI Code of Ethics (§219.11) and the risk assessment and impact assessment required before deploying a "heightened scrutiny" AI system used as a controlling factor in a consequential decision, such as admissions, grading, or discipline (§§219.20–219.24);
- Texas Administrative Code 202 (TAC 202), Information Security Standards;
- The Family Educational Rights and Privacy Act (FERPA), which protects student education records;
- House Bill 1481 (89th Legislature), Texas Education Code §37.082, which restricts student use of personal communication devices during the school day; and
- The Digital Millennium Copyright Act of 1998 (DMCA) and Title 17, United States Code, which govern copyright.

VIOLATIONS

A student's computer use privileges may be suspended immediately upon the discovery of a possible violation of this Standard. Violations of this Standard will be dealt with in the same manner as violations of other College academic policies and may result in termination of enrollment. 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 the above standards may constitute a criminal offense and may be investigated by Campus Police, Information Technology Services, and the Vice President of Student Services.