

	ADMINISTRATIVE PROCEDURE MANUAL	
Section Title: Technology Use Standard and Agreement - Community	Number: cr-07	Page: 1 of 4
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 community members on the acceptable use of the college’s technology resources.

1. Background

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 only allowed access within Alvin Community College’s Library and through the ACC Guest Wi-Fi.

All community members are responsible for using college computing resources in an effective, efficient, ethical, secure, and lawful manner. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as possible legal sanctions under Federal, State, and local law.

2. Users Agreement

All community member users of College 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, community member users agree to comply with this Standard and supporting procedures and guidelines.

3. Rights and Privileges

The computer systems are owned by and operated by Alvin Community College. 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.

4. Usage

Users are not to attempt to access, search, or copy technological and/or information resources without the proper authorization. Users are not to test or attempt to compromise internal controls, even for perceived purposes of systems improvement.

5. 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of authorship” for their intellectual works that are “fixed in any tangible medium of expression”, both published and unpublished (Title 17, United States Code).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 may lose the privilege to access the Alvin Community College computing resources.

6. The Internet

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 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.

7. Wireless Network Access

The Alvin Community College wireless network space is open to College faculty, currently enrolled students, staff, and members of the community. Access to college network systems over WiFi is restricted to authorized college employees.

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.

8. General Provisions

- a. Community members wishing to use Library computing resources must sign in with Library staff and agree to the terms of this document.
- b. Currently enrolled students are given preferential access to Library resources. In the event that resources are reaching capacity, community members may be directed to allow students access to workstations and denied access until adequate resources become available.
- c. The following actions (including but not limited to) will result in 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 self-replicating or similar nuisance program (e.g., virus, Trojan horse), whether or not they are destructive in nature.

9. Maintenance

The responsibility for maintaining the campus computing environment rests with Information Technology Services.

10. Violations

Upon the discovery of a possible violation of this Standard, a community member's computer use privileges may be suspended immediately. Violations of some of the above standards may also constitute a criminal offense and will be investigated by Campus Police and Information Technology Services.