TECHNOLOGY USE

Approved by: Technology Committee

History: Updated 1997 | 2021 | 2022 | 2023

Related Policies: Accessible Technology Policy

Related Forms, Procedures and References: Tech Services | Residence Hall Tech Services (https://www.alverno.edu/Tech-Services-ResLife/) | EIT Accessibility Contact Form (https://docs.google.com/forms/d/1S_KE81DPUzTvKfhFpKr80iRlET3ab2_jZaT89U8cX5g/viewform/?edit_requested=true)

For Questions Contact: Technology Services | 414.382.6336 | RC 109B | helpdesk@alverno.edu

Overview

Alverno College is committed to providing technology resources to support students, staff, faculty and other qualified members of the Alverno community in the educational, administrative, and related social, personal and community activities and functions of the College. This set of policies is designed to provide all users with information to facilitate effective use of technology at Alverno. Authorized users are permitted to access appropriate areas of these resources. Access must follow federal Family Educational Rights and Privacy Act Policy (FERPA) Guidelines. Please refer to the policy in the *Student Handbook* or Alverno & You. *Note: when discrepancies between printed and electronic editions of an official document arise, the document with the most current date takes precedence unless specifically noted. It is your responsibility to stay current with these policies. The most recent version of this policy can be found online* (https://www.alverno.edu/media/alvernocollege/technologyservices/pdfs/TechnologyUsePolicy.pdf/ (http://www.alverno.edu/techserv/departmentinfo/missionpolicies/)).

We ask that you use the technology resources provided by Alverno, whether on or off campus, in a manner consistent with the purpose and the principles of the College. Each user is responsible for following the policies in this document. Since technology environments change rapidly, this document is subject to change. These policies do not replace, but supplement, policies detailed in the *Alverno College Catalog, Alverno & You, and The Alverno Educator's Handbook*.

Responsibility of Users

This policy applies to students, staff, faculty, and other guests of the Alverno community. By using the technology resources of Alverno College, you agree to and accept the responsibilities described in this and other Alverno documents. In general, you agree to follow appropriate *Ethical Conduct*, to maintain a *Respect for Others*, and to assist in maintaining the *Security* of the information available. The use of technology resources at Alverno College is a privilege, not a right. Inappropriate use of resources may result in cancellation of those privileges or other disciplinary action. Inappropriate use may encompass behaviors not described in these guidelines.

Summary of Alverno College Technology Use Policies

Ethical Conduct:

- Comply with the Technology Use Policies
- Identify yourself and your affiliation accurately
- Be responsible for your actions
- Use Alverno's technology resources for lawful and College-approved purposes
- Do not use offensive communications or materials

Respect for Others:

- Protect personal information
- Respect fair use guidelines for copyrighted material and intellectual property
- Be aware of what electronic network communication is not allowed (i.e. chain letters, unsolicited advertisements, spamming/mail bombing, phishing scams)
- Do not share confidential information
- Use the Alverno College name only for official business or with permission

Security:

- Do not distribute your password or the password of another person. Do not use another person's password
- Password change is required every 180 days. Accounts must be configured to use multi-factor authentication (MFA)
- Report violations
- Do not send confidential information electronically in an unsecured fashion. Do not send unauthorized confidential information
- These policies apply whenever you are using Alverno resources
- An antivirus application, with current virus definitions, must be installed on a personally-owned computer when connecting to the campus network. In addition, the devise should have a current operating system (OS). OS and applications should be updated and patched regularly

Accessibility:

- Electronic and information technology (EIT) must be designed, developed, managed, acquired or procured to be accessible to the widest range of users possible, in accordance with federal and state law.

Ethical Conduct

Compliance with Technology Use Policies – You are expected to comply with the terms of the Alverno College Technology Use Policies and to report violations of the policy to the appropriate College personnel (please refer to the last page). This policy applies when accessing the resources of other institutions through Alverno College. Other institutions may have more restrictive use policies and you must abide by those policies as well as the policies of Alverno College.

Compliance with Alverno Library Policies - All Alverno students, faculty, and staff are issued library barcodes when they receive their college identification cards. By using your library barcode to borrow materials or to access electronic resources through the library web site or TOPCAT (the library's online catalog) you agree to abide by the Alverno Library Circulation policies. You are responsible for all materials and equipment borrowed on your library barcode including any replacement costs and processing fees for lost or damaged items, or for any overdue fines for late materials or equipment. The borrower's agreement covers any items borrowed from the Alverno Library, the Media Hub, any of the SWITCH

libraries, or through Interlibrary Loan or Infopass transactions. In the event any legal action is taken, you agree to pay all reasonable collection costs, including attorney's fees and other charges necessary for the collection of any amount not paid. For a detailed list of the Alverno Library Circulation policies, please see https://www.alverno.edu/library/policies (https://www.alverno.edu/library/policies/).

Self-Identification - Identify yourself and your affiliation accurately in electronic and verbal communication. Concealing your identity or using the identity of others is fraudulent, irresponsible and a serious violation of this policy.

Personal Responsibility - Be responsible for your actions, as an Alverno College community member and as a member of the global community. Personal conduct carries a burden of responsibility and you must be aware of, and accept responsibility for, the consequences of your actions. This includes accepting responsibility for protecting your own work. Maintain backup copies of important work and change your password often., at least every 180 days. Alverno will email reminders and require a password change after 180 days.

Lawful and Permitted Purposes – Use Alverno's technology resources for lawful and College approved purposes. Approved primary purposes include teaching and learning, and official College business. Permissible secondary purposes include College-related social, personal, and community functions and activities. Use of the technology resources for secondary purposes is always subordinate to use for primary purposes and must not involve significant use of technology resources, direct costs, or substantially interfere with the performance of teaching and learning, official College business, and administrative matters. The use of resources for purposes not specifically permitted by the College, or assisting others in infractions of College policies, is a violation of this policy.

No Offensive Communications or Materials - Maintain a high standard of conduct in your communication. You are a member of the Alverno community and your actions reflect on all students, faculty and staff. Accessing, or assisting others in, downloading, uploading, transferring, posting, displaying, or printing of sexually explicit or pornographic images of any kind, or materials considered obscene, vulgar, harmful, hateful, harassing, threatening, defamatory, demeaning, or otherwise objectionable is a violation of College policy. Sending material that is abusive, offensive or unwanted may disrupt the work of others and is a violation of the policy.

Social Media - Social media is designed to disseminate information through social interaction. Alverno College believes in interaction with others to achieve goals, resolve conflicts and build relationships. Social media sites, such as LinkedIn, Facebook, Twitter, YouTube, Snapchat, Instagram, TikcTok, WhatsApp and many others allow faculty, staff and students to develop social interaction skills and to stay connected in their personal and professional lives. This policy has been created to ensure operation is in accordance with College policy and represents the College's best interest.

Faculty, staff and students are expected to act responsibly and to follow the same behavioral standards online as they do in real life situations, as described in detail above. Information and photos posted online are public information and inadvertent use of identifying information could be in violation of FERPA or HIPAA regulations. Students, faculty and staff are encouraged to be prudent when posting information on social media sites. Alverno College does not routinely monitor online communities, however, pictures and information brought to the attention of the College describing or documenting behavior considered to be in violation of College policies, such as those listed on page one of this document or in other official college handbooks, on campus or off campus at a College sponsored event, will be subject to further investigation. If such an investigation finds that any College policies have been violated, appropriate disciplinary action will be taken. Contact the Marketing and Communications department for a copy of Alverno's Social Media Guidelines.

Respect for Others

Personal Information of Other Individuals - Protect personal information of other individuals when disseminating electronic information. If you observe an individual's personal information being disclosed in an objectionable manner, you are required to report it to the appropriate personnel/supervisor.

Copyright and Intellectual Property -

- Respect fair use of copyrighted material and intellectual property. Copying of materials, including passwords and files, which belong to others, constitutes a breach of the policy. Note that unauthorized duplication or transmission of copyrighted or other proprietary content could subject you to criminal prosecution as well as personal liability in a civil suit. Alverno College does not require, request, or condone unauthorized copying or use of computer software, scanned or digital images, audio or video files, music, movies, television shows or other digital video media by College employees or students. The College will not provide legal defense for individuals who may be accused of making/downloading such unauthorized copies of files even if these individuals maintain that such action was taken in the course of their employment by or enrollment at Alverno College. If the College is sued or fined because of unauthorized copying or use, it may seek payment from the individuals as well as subject them to disciplinary action. More information can be found on the Library's website: https://libguides.alverno.edu/copyright/basics (https://libguides.alverno.edu/copyright/basics/).
- Use software owned or licensed by the College in accordance with the applicable license. Viewing, modifying, or damaging information without authorization (including intentional introduction of viruses or unauthorized access) is unethical, may be unlawful, and is in violation. Users should assume that copying of software for use on an additional machine is prohibited unless specifically granted permission by college personnel authorized to make that decision.
- You may, in accordance with College policies, electronically distribute or duplicate information, software, video, graphics, photographs, music, and other material that does not fall under copyright, trademark, or other intellectual property protection.
- Use of copyrighted material for which permission has been granted by the owner must include a phrase similar to "Copyright owned by [owner's name, date]; used by permission."

Needs Of Others For Resource Access - To minimize demands on Alverno's technology resources and maximize the availability of those resources, you are expected to refrain from activities that generate excessive network traffic. These include but are not limited to:

- Peer-to-Peer sharing of data using applications such as, FrostWire, Deluge, uTorrent, qBittorrent, TPB, Freenet, etc.
- Mining cryptocurrencies using Alverno resources is prohibited.
- Use of web cams are acceptable when used for teaching and learning purposes. Usage should be limited to activities that fall within the guidelines of the Ethical Conduct and Respect for Others sections of

this document. When using personal web cams, users are expected to observe the privacy of others as well as understand that their actions represent the College.

- Chain letters and pyramid schemes;
- Inappropriate or unsolicited advertisements (advertisements, promotional material, or other types of solicitation must have prior approval by Student Affairs or other appropriate College authority);
- Posting irrelevant or inappropriate electronic messages to multiple recipients ("spamming");
- Multiple unsolicited electronic messages to a single recipient ("mail bombing"). Mail lists (electronic mail) may be maintained that allow Alverno users to subscribe/unsubscribe to electronic mailings. These lists would fall under the category of solicited advertisements. Electronic mailings to all individuals on such lists require prior approval or a standing authorization for such mailings from Student Affairs or a Vice President. The names and e-mail addresses of individuals on mailing lists may not be distributed outside the Alverno Community;
- Devices that do not support WPA2-Enterprise (802.1X) authentication are not allowed to connect to our secure wireless networks. An open, unsecure Guest network is available with Internet only access, but a guest username and password is required to connect. We also provide a less secure, Internet access only, wireless network for our residents (device registration required) to connect "home" devices that do not support WPA2-Enterprise;
- Personal routers or access points are not permitted on Alverno's network.

In addition, you are expected to install and run a legal, fully functional antivirus program and to perform regular virus definition updates as well as periodic system virus scans.To prevent a widespread network disturbance, any machine found to be infected with a virus, worm, etc. will be disconnected from the campus network immediately upon discovery, and will remain disconnected until deemed "clean" by the Technology Services department. This information also applies to any remote connections made to the campus network.

*Alverno College installs antivirus software on all college-owned computers. If you connect to Alverno's network using your personal device (either on campus or through remote access), you must have an antivirus application installed with current antivirus definitions.

Confidential Alverno Information - Respect the confidentiality of institutional information. Some Alverno College materials are not intended for audiences outside the institution, could be taken out of context, may be Alverno copyrighted, or are legally confidential. If you access confidential information unintentionally, please contact the owner of the information, network security coordinator, and/or other appropriate personnel as soon as possible. In addition, you are responsible for College-owned information stored on your personally owned device such as a USB drive, tablet, laptop, smartphone, home computer, etc. You should take appropriate security measures, to protect the data and ensure that FERPA and HIPAA laws are followed. Alverno data should be stored in accordance with Alverno's Data Protection Policy and Guidelines.

Use of Alverno College Name – The Alverno College name may only be used in an official context for College business. To avoid misrepresentation of Alverno College, do not use the Alverno College name or any symbol, graphic, text, or logo associated with Alverno College in a manner implying endorsement of any political, social, or commercial activity or in a context that implies official endorsement by the College without prior written approval of Student Affairs, Marketing Communications, or other appropriate College authority. Individuals who, through their employment or other established association with the College, represent Alverno in an official capacity are not required to obtain written permission but should ensure that the College is represented in an appropriate manner.

Security

Multi-Factor Authentication (MFA) – Alverno College utilizes MFA in order to secure logins and protect sensitive data and/or intellectual property. Faculty, staff and students are required to register for MFA to ensure that their account has two or more authentication methods.

Passwords – Change your password often (required every 180 days). A password is your "key" to Alverno's technology resources. When choosing a password, use the following guidelines:

- Use at least eight characters (a combination of letters, numbers and special characters); cannot reuse the last five passwords
- Pick a password that is easy for you to remember, but that others would not likely be able to guess;
- Do not write down your password because someone might see it and use it;
- Choose a unique password (not the same password as the one you use for automatic teller machines or online banking).
- NEVER share your password with other individuals. Remember they could use your password, delete your files, impersonate you, or change your password to lock you out.

Access Restrictions - Do not distribute your password or the password of another user. Do not use other's passwords. These are serious violations of this policy. Attempting to disable or determine an access password (or assisting others in doing so) is prohibited. Such activities threaten the work and privacy of many individuals. Respect the restrictions imposed by the technology resources of other individuals and organizations. Do not attempt to circumvent access restrictions. Violation is grounds for immediate suspension of access privileges or other disciplinary action.

To maintain network security, accounts are deleted on a regular basis. Account deletion includes but is not limited to removing access to Alverno's network, deleting files in individual home directories, cloud storage (H drive, OneDrive, Google Drive, OneNote, Moodle, etc.) and deleting email.

- Student accounts are active for six (6) months after graduation. After that time, the account is deleted.
- Accounts for students whose status changes to Official Withdrawal or Dismissed are deleted shortly after the status change is made.
- Accounts for Students on Leave remain active. If a student's status changes from Student on Leave to Official Withdrawal, the account is deleted.
- Employee accounts, including student employee accounts, will be disabled/deleted upon separation of employment.

Use of Others' Technology Resources - When using the technology resources of others through Alverno's facilities, these policies apply. Information providers or networks outside Alverno College may also impose their own conditions for use and you are responsible for following any additional restrictions.

Monitoring and User Privacy - Treat all electronic communications as potentially accessible by others. Please consider this before sending

confidential information electronically. Alverno College considers electronic mail and other electronic information to be private, although it is Alverno property. Information must be accessed by system personnel for the purpose of backups, network management, troubleshooting and maintenance. In circumstances where an account or system is suspected of suspicious behavior or breach, or being used in violation of the Technology Use Policy or other campus policy, federal or state law impacts system integrity, the Campus Network Security Team, Director of Human Resources, Dean of Students or other person of authority may authorize system support personnel to monitor the activities of a specified account or computer system and to search electronic information stored in that account. The authority for this search must be requested on an account-by-account basis and monitoring will be restricted to the specified account. If this search provides evidence of a violation, the account will be disabled and action will be taken with the proper authorities.

Disciplinary Actions

Alverno College reserves the right to revoke the technology access of any user at any time regardless of enrollment or employment status. Procedures for disciplinary actions involving students are outlined in the Student Code of Conduct: Process and Sanctioning Guide; disciplinary procedures for faculty and staff are described in Alverno & You. Alverno College reserves the right to take the following actions in response to technology violations:

- Send a verbal, written, or electronic mail warning;
- Allow only restricted access privileges;
- Suspend computer or other technology access for a temporary time;
- Revoke all computer or other technology privileges;
- Assign an “Unsatisfactory” (if violation relates to student course work);
- Allow other discipline up to and including dismissal from the College or termination of employment.

Minor infractions of the Technology Use Policies, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally. This is done through electronic mail or in-person discussion and education. Repeated minor infractions or more serious misconduct may result in additional disciplinary actions.

More serious violations include, but are not limited to:

- Unauthorized use of computer resources
- Copyright violations
- Attempts to steal passwords or data
- Transfer or display of offensive material
- Harassment, or threatening behavior
- FERPA or HIPAA privacy rule violation

In addition, offenders may be referred to their supervisor or other appropriate College offices for further action. If the individual is a student, the matter may be referred to the College Community Relations Board for disciplinary action. Any offense which violates local, state, or federal laws may result in the immediate loss of all technology privileges and will be referred to the College Community Relations Board (students), your supervisor (faculty/staff) or other appropriate College offices and/or law enforcement authorities.

In cases where the integrity or functionality of the network or a multi-user system is in jeopardy, College personnel involved in network security are authorized to take immediate steps to prevent further damage - up to and including disabling user accounts and disconnecting a user’s computer from the campus network.

Technology Use Resources - When you want to...

- **Open an account** - Technology Services automatically creates student accounts. Supervisors of student employees can request accounts at: https://intranet.alverno.edu/files/galleries/student_employee_account_request_form.pdf.
- **Obtain technical assistance** - Technology Services, Computer Center, 414-382-6336 or 414-382-6700 (Available 24x7; after-hours and weekend/holiday support is provided by a third-party organization)
- **Report a policy infraction** (non-security related): Dean of Students, 414-382-6116
- **Report a security violation** - Campus Network Security Team Coordinator, network-security@alverno.edu