General IT Campus Policy

https://www.miles.edu/it-support#chapter=chapter-1681-General-IT-Campus-Policy

Computer and Network General Use Policy

To fulfill our mission, Miles College uses a wide variety of information technologies to assist in serving the campus. The Information Technology Policy provides the campus community with guideline for the proper use of the Office of Information Technology (IT) computer hardware, software, email, and Internet service.

Any use of Miles College information technology systems contrary to this policy may lead to a withdrawal of access. Abuses that may result in termination of access rights include, but are not limited to, knowingly downloading illegal software or music, engaging in the abuse of a fellow member of the Miles College community via the Internet or social media outlets, and sending spam to Miles College email addresses.

These guidelines are designed to inform faculty, staff, and students on their responsibilities as it relates to the use of Miles College technology resources. Information technology (IT) resources is interpreted to include all Miles College system computing and telecommunications facilities, equipment, hardware, software, data, systems, networks and services which are used for the support of teaching, research and administrative activities of the College.

It is the responsibility of each faculty, staff, and student to follow the following policies. The responsibilities are shared with them during faculty/staff conferences, divisional meetings, new student orientation, and in the classrooms. This policy is also available online.

- Understand and follow the IT policies in this document.
- Use the computer systems properly.
- Protect the integrity of the systems by treating equipment with care and respecting IT security measures.
- Call the helpdesk when a problem occurs.

It is the obligation of the IT staff to:

- Educate the campus community about any IT questions or concerns.
- Follow a process that addresses IT needs in a timely manner.
- Provide faculty, staff, and students with working equipment that helps to meet their needs.
- Respect faculty, staff, and students' privacy for all information they store in the IT systems.
- Respond to IT Help Desk calls in a timely manner.

Student Training in Technology

The Miles College Office of Information Technology assists in providing training in the use of technology through the required Computer Literacy Course in which all students must enroll as part of general core requirements. It provides a comprehensive overview of computer technology, familiarizes students with basic terminology, and prepare students to understand and utilize computers in their personal and professional lives.

Faculty Access and Training in Use of Technology

The Miles College faculty has desktop computers and is provided with training in the use of applications. The College maintains technology appropriate to meeting the learning outcomes of its programs as well as to ensure faculty access to technology.

Management and Access Controls

Each IT resource has a designee who is responsible for its security and management. Each authorized user of a system has a unique login ID. Any ID which is used to access a system and does not provide a unique user identification, has access only to specific, restricted system resources. Access to services and/or resources are suspended, and the appropriate account deleted when there is no longer a business or academic need for access. Employees are required to remove any personal data from Miles College computer systems prior to their last day at Miles College. The deprovisioning of the account is performed in a manner proportionate to the level of risk posed by such access, including immediate suspension of access and privileges and deletion of the account if necessary.

When an employee is terminated, that responsibility falls upon the department and the user's supervisor to report termination. Information Technology, upon an employee's termination and departmental request, stores files on a network drive and makes it available to the new departmental data owner for a period of one (1) year, unless a request is otherwise made, at the end of which the files are purged from the system. By default, IT will keep email, and user account is disabled.

Access control procedures is used to authenticate all users who access each system. Such controls include, at a minimum, a login ID and a response mechanism (such as a password) for each user. All user accounts are required to change passwords periodically. The frequency is determined by the enforced length and complexity of the password combined with the sensitivity of the data protected, in accordance with industry standards and guidelines published in the security website.

Access rights and privileges for all authorized users are maintained and managed so as to secure access to data in a manner appropriate to the needs of the user and the value of the data. Confidential data is protected against unauthorized access regardless of form, computing environment or location.

Hardware (Including hardware issued and used offsite)

- Installing and Removing Hardware – Users are not authorized to attach/detach or install/uninstall any computer components without authorization from their Division Chair and involvement of IT staff. This includes keyboard, mouse, printer, modem, monitor, internal boards, or components. The Office of Information Technology is responsible for assigning computer components to specific computers.

- Storing Data – Users with the need for an extraordinary amount of data storage should notify their Division Chair who will then work with the IT staff to meet the user's needs. If portable media containing electronic protected health information is generated, the user must take the responsibility to store the media in a secured, locked location and dispose of the media per the media disposal guidelines when no longer needed.

- Acquiring and Disposing of Computer Hardware – The purchase of any computer hardware or the disposal of old computer hardware is done only with the approval of the Director of Technology and involvement of IT staff. Please check with the IT staff on proper disposal of removable media (CDs or floppy disks…) containing confidential information.

Software

- Installing Software – It is the responsibility of the Office of Information Technology to install any software on Miles College computers. User must submit a "User Request Form" found on the IT page of the Miles College website, to have any program installed on any Miles College equipment by the IT staff.
- Unauthorized Downloadable Software – The use of unauthorized downloadable software is prohibited. Downloadable software such as freeware, shareware, program demos, surveys, advertising, training, Internet browsers, copyrighted data, fonts, personal digital images, graphics, and personal photos should not be downloaded without prior approval.
- Software Licensing Compliance – Violation of any software licensing agreement, copyright, or other intellectual property rights of third parties is strictly prohibited. This includes, but not limited to, computer software/data or related manuals and materials. Contact the Office of Information Technology for more information about software licensing agreements.

Internet and Email

- Internet and Email Usage – The computer system, Internet and email system are to be used for college business purpose only; however, the organization realizes that occasionally it is necessary for employees to use the Internet for important personal issues, but such usage must be kept to a minimum and all computer use rules must be followed. Some examples of limited personal use may be to access other email accounts, bank accounts, and to verify travel plans.
- Your email account is the official means of communication from the College. You are expected to check it regularly.
- All restricted information must be approved, encrypted, and password protected.
- Mass emails should only be used for official college events or communications. The mass email system should not be used for private marketing, solicitation, etc. without prior approval.
- It is prohibited to use the Miles College email system to create, forward, and/or distribute any material that is disparaging or otherwise offensive.
- Viruses – The IT network or any computer resources cannot be used to download or distribute pirated software or data, or to propagate any virus or variant thereof. Instant messaging/chat rooms and the like are expressly prohibited to all employees unless specifically authorized otherwise.

System Security

- Shutting Off Computers – Users have the responsibility to sign off the computer after they are done using the computer or whomever they need to leave the computer for an extended period. When leaving a computer unattended, lock/log off the computer.
- Virus Scan – Disks, removable media, and drives from any outside source have to be scanned for viruses prior to opening the contents on the disk/removable media/drives.
- Laptops – Laptops need to have virus software updated regularly. The Office of Information Technology will provide users with practical avenues to accommodate anti-virus software updates.

Harassment

Harassment of any individual or group through email, websites, or any other online means is prohibited. Harassment takes many forms. In general, it creates an uncomfortable or hostile environment for the individual or group who is being harassed. If you send, an email message to another person and make unwanted sexual advances, or if you send unwanted digital messages, or if you send many messages to another person, you are harassing that person.

Monitoring and Enforcement

The Miles College Office of Information Technology actively monitors network and network resources. Most monitoring activities are routine, and allow the IT staff to detect, diagnose, and fix the normal day-to-day problems associated with operating a complex network. Monitoring also ensures that the network is used for is intended purpose-academics and academic support-and safeguards the College against legal risk.

When Miles College believes that technology, resources are being:

- Misused
- Inappropriately used
- Illegally used
- Used in a way that compromises or threatens the functioning of the system
- Used in conflict with College policies or local, state, federal, or international law

Miles College reserves the right to instigate, and to take whatever action is necessary to maintain system integrity and security.

Miles College may review individual IT records to the extent necessary to assess the problem and determine responsibility. Miles College also reserves the right to delete files, programs, network connections, and/or user accounts.

Both network and individual user logs may be examined. This includes the logs on personal computers or servers that are attached to the College network, whether they are owned by the College or by other parties.

Abuse of technology privileges may result in appropriate disciplinary action. In many cases, the user is given a warning. Cases involving students may be referred to the Office of the Dean and Vice President of Student Affairs. If the user violates our policies more than once, then this may result into the account or computer losing network privileges.

The College may suspend or revoke user email or network privileges. In cases of illegal activity, the College may refer the matter to law enforcement authorities.

Finally, the College reserves the right to respond to legally mandated requests for technology records. For example, if a law enforcement agency is investigating allegations of copying and distribution of copyrighted material, and serves a court-approved search warrant upon the College, the College is obligated to permit the search.

Prohibited Uses of Miles Computers

- Do not use the video feature on your PC unless you are using it for web cast based training/teleconferencing that is relevant to your work.
- Offensive or Inappropriate Information – Preparing, displaying, or transmitting messages, pictures, or information consideration offensive or inappropriate including, but not limited to, content pertaining to race, ethnicity, religion, age, gender, veteran status, sexual orientation, or sex.
- Copyright – Copying, replicating, or transmitting documentation, software, or other information in violation of copyright laws.
- Network – Disabling or overloading any computer network or circumventing any system designed to protect the privacy or security of another user.
- Unauthorized Persons – Providing IT systems access to unauthorized persons.
- Unauthorized Access – Gaining unauthorized access to electronic information and communication systems.
- Inappropriate Websites – Accessing websites including but not limited to pornography, gambling, gaming, dating, shopping, music file downloading, job searching, chain letters, and etc.

Peer-to-Peer File Sharing (P2P)

- Unauthorized peer-to-peer (P2P) file sharing on college campus is receiving increasing attention from the entertainment industry, the media, and the United States Congress. Although P2P file sharing on college networks is not unlawful, such activity is not necessarily harmless [or without harm] especially as it can lead to a violation of the federal copyright law. Indeed, many student using popular software, such as Ares, Direct Connect, Morpheus, LimeWire, and Gnutella, intentionally or advertently infringe on copyrighted works relating to music, movies, computer software, video games, and photographs. Lawsuit filings indicate copyright owners are taking the offensive against infringements on their protected works. Students need to know their rights and responsibilities, and their potential liability for unlawful P2P activities.

- Miles College does not actively monitor illicit or inappropriate activities, nor is it under obligation to defend or accept responsibility for its students' illegal actions in the P2P context. Miles College expects our user's community to act in a proper and responsible computing manner and to the extent possible attempts to thwart illegal file sharing. However, if illegal or inappropriate activities are brought to our attention, the College takes all reasonable and appropriate actions.
- Avoid downloading, distributing or possessing copyrighter material over the Internet and the College internal network unless you have received explicit permission from the owner or their official representative, or have paid an access or license fee to obtain the material. If you are using a peer-to-peer application, you should remove it from your system prior to connecting the College's network. If you do not remove the application, you should ensure your system is set to prevent the application from acting as a provider or unlicensed materials to other users. Failure to restrict the application, whether you are aware of the violation or not, result in the College's information technology unit removing your machine from the network until the copyright violation is rectified.

Spam Prevention

- It is the responsibility of each computer user to take steps to safeguard against increasing the amount of spam that comes into the College.

Connection from On-Campus

- Computer network access is provided to students across the campus. The whole campus, including the residence halls is equipped with 802.11 b/g/n wireless network coverage.
- To access the Miles/Miles Student wireless network, your computer must be equipped with a wireless network interface card (NIC) and configured for support WPA2 certification. The wireless key is provided by the Office of Information Technology.
- Personal Hubs, routers, or wireless access points are not allowed.

Disclaimer

No responsibility is accepted for any damages, direct or indirect, howsoever caused, arising from any user's use of Library computers or associated Internet access.

Questions on the above policy can be sent to it_support@miles.edu or call 205.929.1498.