

WILBRAHAM & MONSON ACADEMY

423 Main Street Wilbraham, Massachusetts 01095 Phone 413.596.6811 Fax 413.596.2448

Web site: www.WMA.us

Acceptable Use of Technology Policy

Introduction and Overview

Access to information technologies is integral to the educational mission and purpose of Wilbraham & Monson Academy (WMA). We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our school. This Acceptable Use of Technology Policy (AUP) provides expectations for the use of technology as it affects our school and educational community. The school's computer network is provided for limited educational purposes, not as a public access service.

Due to the evolutionary nature of technology, it is imperative for Users to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all users to employ their best judgment when it comes to the use of school technology and keep in mind that our policies related to technology are not meant to supersede our other school policies, but rather to compliment them. Although our school provides certain technologies, we recognize that members and guests of our community also have their own technology devices that they bring to our campus and school events. Our policies address the appropriate use of both technologies provided by the school and personally owned technological devices. Please read the policies below before using our network and computers, because by using our technology you agree to be bound by the terms, conditions and regulations below.

Scope and Acknowledgement

This AUP applies to all students, all faculty and staff members, and all visitors to campus (both adults and minors) including parents and sub-contractors, herein after Users.

All people visiting our campus are also subject to the terms and conditions of this AUP.

All students and their parents or guardians must sign for their acceptance of this AUP **before** they can utilize any school technologies. This signature is required on an annual basis at the beginning of every school year.

All Wilbraham & Monson Academy employees must sign for their acceptance of this AUP **before** they can utilize any school technologies. This signature is required one time only for new employees unless the form is updated in a subsequent year.

All students and faculty members participate in a presentation about the appropriate use of our technology resources and acceptable and unacceptable behaviors related to technology at the start of every school year. This presentation is repeated in subsequent years, even if individuals are returning.

Use of school's Name and Image

Our institution prides itself on its reputation for excellence; therefore, you may not use the school's name, logo, mascot or other likeness or representation on a non-school Web site without express permission from our institution. This includes pictures of anyone wearing clothes with the school name, crest, emblem, or logo. This also includes listing our school name or our employees on a social networking profile, a dating Web site profile, or a Web site that involves rating or judging of another member of the WMA community.

Technology as a Privilege

The use of school and personally owned technology on school property or at school events is a privilege not a right. This privilege comes with personal responsibilities and if you violate the responsible use of any school technologies, your privilege may be revoked and/or suspended and you may be subject to disciplinary consequences.

Our school provides sufficient information technology resources for each user for regular academic pursuits and campus living. If a particular research project requires additional resources, the Information Technology (IT) department works with Users on a case-by-case basis to provide additional resources.

Personal Responsibility

We expect everyone to act responsibly and thoughtfully when it comes to using technology. Technology is a finite, shared resource offered by the school to its community members. Users bear the burden of responsibility to inquire with the IT department or other school administrator when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

Honesty and Personal Integrity

Do not pretend to be someone else online or use someone else's identity without express permission from that person and/or his/her parent/guardian if he/she is a minor.

Do not use, post, or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than yourself. This includes intellectual property that you were given permission to use personally, but not publicly.

A work or item is copyrighted when, among other issues, one person or one group owns the exclusive right to reproduce the work or item. Songs, videos, pictures, images, and documents can all be copyrighted. Copyright infringement is when you violate copyright law and use or reproduce something without the authority to do so. Make sure to appropriately cite all materials used in your work. Do not utilize someone else's work without proper permission.

The above behavior will be considered a violation of school policy as well as state and federal laws.

Definitions and Terms

Bandwidth: Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.

Bullying: Bullying is the repeated use by one or more students of a written, verbal or electronic expression or a physical act or gesture or any combination thereof, directed at a victim that: (i) causes physical or emotional harm to the victim or damage to the victim's property; (ii) places the victim in reasonable fear of harm to himself or of damage to his property; (iii) creates a hostile environment at school for the victim; (iv) infringes on the rights of the victim at school; or (v) materially and substantially disrupts the education process or the orderly operation of a school. For the purposes of this section, bullying shall include cyber-bullying. (M.G.L. c. 71, § 37O)

Cyber-Bullying: Cyber-bullying is bullying through the use of technology or any electronic communication, which shall include, but shall not be limited to, any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications. Cyber-bullying shall also include (i) the creation of a web page or blog in which the creator assumes the identity of another person or (ii) the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying. Cyber-bullying shall also include the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying. . (M.G.L. c. 71, § 37O)

Downloading: Downloading refers to the transfer of data from an Internet computer off campus to a computer on campus. This includes indirect downloading such as, but not limited to, streaming music and/or video, and using voice and/or video communication.

Internet: The Internet connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.

Network: The school's network is defined as our computers and electronic devices such as printers, fax machines, scanners, etc. that are connected to each other for the purpose of communication and data sharing.

Personally Owned Device User: For the purposes of this AUP, personally owned device user refers to anyone who utilizes their own technology on property owned or controlled by the school or at a school-sponsored event.

PDA: PDA stands for personal digital assistant, an electronic device which provides some of the functions of a computer, a cell phone, a music player, and a camera.

Technology: Under this policy, technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, stereo or sound systems, digital media players, gaming consoles, gaming devices, cell phones, personal digital assistants, CDs, DVDs, camcorders, calculators, scanners, printers, cameras, external and/or portable hard drives, modems, Ethernet cables, servers, wireless cards, routers, and the Internet. School technology refers to all technology owned and/or operated by the school.

User: For the purposes of this AUP, user is an inclusive term meaning anyone who utilizes or attempts to utilize, whether by hardware and/or software, technology owned by the school including students, faculty members, staff members, parents, and any visitors to the campus.

Expectation of Privacy/Confidentiality

The school reserves the right to monitor and track all behaviors and interactions that take place online or through the use of technology on our property or at our events. We also reserve the right to investigate any reports of inappropriate actions related to any technology used at school. All e-mails and messages sent through the school's network or accessed on a school computer can be inspected. Any files saved onto a school computer can also be inspected. Members of the community have a limited expectation of privacy when using their own technology on school property or at school events as long as no activity violates the AUP, law, and/or compromises the safety and well-being of the school community.

Except for instances when the Deans Office contacts parents about a specific disciplinary issue, parents and guardians are not allowed to see the e-mails and other data for their child's technology account at school. In the case of a disciplinary circumstance, the school will determine the appropriate information to share. Otherwise, matters of privacy are between the parent and child.

Respect for the Privacy of Others and Personal Safety

Our school is a community and as such, community members must respect the privacy of others. Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others. Do not misrepresent or assume the identity of others. Do not re-post information that was sent to you privately without the permission of the person who sent you the information. Do not post private information about another person. Do not use another person's account. If you have been given an account with special privileges, do not use that account outside of the terms with which you were given access to that account.

Do not voluntarily post private information about yourself online, including your name, your age, your school name, your address, your phone number, or other identifying information.

School-Provided Technology Resources

Network storage is a finite school resource and we expect Users to be respectful of other Users and limit the amount of space and memory taken up on school computers and on the school network.

All students and employees are provided with a school e-mail account. All e-mails sent from this account are representative of the school and the user should keep in mind school policies regarding appropriate language use, bullying, stalking, and other policies and laws. E-mail accounts are subject to monitoring and members of the community have a limited expectation of privacy when using their own technology on school property or at school events as long as no activity violates policy, law, and/or compromises the safety and well-being of the school community.

Users are sharing resources such as bandwidth and server space with others and downloading large files utilizes finite resources. Abusing these resources can result in the loss of this privilege. Please delete old e-mails and save large attachments elsewhere to limit the amount of storage space your e-mail account is using.

This institution has wireless Internet that is protected by a password. If you desire to connect your laptop or hand held device to the Internet, you must contact a member of the IT department. Unauthorized access is forbidden, which includes providing your access to unauthorized persons.

The school provides individual technology accounts to keep track of technology use. Users must log off when they are finished using a school computer. Failing to log off may allow others to use your account, and Users are responsible for any activity that occurs through their personal account.

Filtering

Our school adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act. This means that all access to the Internet is filtered and monitored. The school cannot monitor every activity, but retains the right to monitor activities that utilize school owned technology. By filtering Internet access, we intend to block offensive, obscene, and inappropriate images and content, including pornography.

Purposes and Use Expectations for Technology

Members of the WMA community may utilize school technologies for some recreational uses, keeping in mind that school technology resources are both shared and finite. These resources include, but are not limited to, disk space, bandwidth, CPU time and effort, printers, faxes, software, and workstations.

Time of Day: Recreational uses of school technology will be limited somewhat depending on Internet site topics and late-night hours for some students.

These hours include, but are not limited to:

Seniors:	Sunday-Thursday	5 p.m.-1 a.m.
	Friday-Saturday	5 p.m.-2 a.m.
Underclassmen:	Sunday-Thursday	5 p.m.-11 p.m.
	Friday-Saturday	5 p.m.-midnight

Activity: Allowable recreational uses of school technology include:

- playing appropriate and non-offensive games
- non-school-related research
- communicating with friends and/or family members
- using voice-over Internet technologies
- updating profiles or accounts on social networking Web sites
- looking at pictures
- similar activities that do not otherwise violate school policy

Bandwidth Used: If your recreational use interferes with another's educational use, you will be asked to refrain from your activity or engage in your activity at a specified time. **If the sum total of all downloading exceeds 500 mb in a single day, the school reserves the right to remove access. Appropriate exceptions can be made by consulting with IT prior to the anticipated use. WMA can provide access to large update files from on-campus servers, removing the need to download from Internet sources. **

Downloads and File Sharing: Users may never download, add, or install new programs, software, or hardware onto school-owned computers, except when the material is for specific academic projects. Downloading sound and video files onto school-owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive. Users may never configure their school computer or personally owned computer to engage in illegal file sharing. The school will cooperate fully with the appropriate authorities should illegal behavior be conducted by Users.

Data and Gaming Devices: Users may play appropriate and non-offensive video games using the school's technology, but may not engage in 'live' interactive online gaming. If a user has been identified as using a large amount of the school's bandwidth or network space to play a video game, the user may be asked to delay his/her game if someone else needs the bandwidth to complete school work. Repeated warnings of bandwidth overuse will result in suspension of privileges. Users may play appropriate and non-offensive computer games using school-owned computers, but these Users may be asked to give up their computer if they are playing a game and another user needs a school-owned computer for school work.

Cell Phones and Personal Electronic Devices

Personal electronic devices such as cell phones, pagers, disc players, and iPods may not be visibly worn, turned on, or in use during the school day, in the dining hall, or during school commitments. For example, they may not be used during the academic day, sports/activities, meals, meetings, or evening study hall.

Recording, Video, and Photography

Digital capturing devices are permitted on campus, but should be used in a safe and appropriate manner within prescribed bandwidth limits.

Social Networking and Web-site Usage

Members of the community may access their profiles or accounts on social networking Web sites through the school's technology, but only after the academic day. Users may be asked to give up the computer if they are accessing a social networking Web site from a school-owned computer and another user needs the computer for academic purposes.

Users may access their own pictures or view other's pictures on photography sharing Web sites such as Photo Bucket, Webshots, or Flickr, but they may be asked to give up the computer if they are accessing a photography sharing Web site from a school-owned computer for non-academic reasons and another user needs the computer for school work.

Users are not permitted to access from the school's technology any Web sites that involve rating or judging of another member of the WMA community. Users may not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

WMA employees are not allowed to 'friend' WMA students, or otherwise establish a direct social link with WMA students on social networking sites.

Communication: Instant Messaging, E-mail, Posting, Blogs

Communication includes, but is not limited to, any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system, including, but not limited to, electronic mail, internet communications, instant messages or facsimile communications. (M.G.L. c. 71, § 37O)

Users may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy others in their community. This is unacceptable behavior known as cyber-bullying and will not be tolerated. Any cyber-bullying, on or off campus, that is determined to disrupt substantially the safety and/or well-being of the school is subject to disciplinary action.

Inappropriate communication in any of the above forms is prohibited in any public messages, private messages, and material posted online by Users. Inappropriate communication includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by Users; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If you are told by another person to stop sending communications, you must stop.

Do not post or send chain letters or spam. Spamming is sending an unnecessary and unsolicited message to a large group of people. Spamming can occur through e-mails, instant messages, or text messages.

Commercial Use

Commercial use of school technology is prohibited. Users may not resell their network resources to others, included, but not limited to, disk storage space. The school is not responsible for any damages, injuries, and/or claims resulting from violations of the AUP. Users who are engaged in fund-raising campaigns for school-sponsored events and causes must seek permission from their advisor before using technology resources to solicit funds for their event.

Computer Settings and Computer Labs

Users are only allowed to alter, change, modify, repair, or reconfigure settings on school-owned computers with the express prior permission of the IT department. This includes deleting cookies and history and re-setting the time and/or date on the computer.

Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited. WMA reserves the right to remove access from any machine found to be spreading harmful software, whether it is intentional or not.

Food and drink are prohibited from school computer labs. Users may not eat or drink while using any school-owned computers or other technologies.

Users may not circumvent any system security measures. The use of Web sites to tunnel around firewalls and filtering software is expressly prohibited. The use of Web sites to anonymize the user is also prohibited. The use of Web sites, both domestic and international, to circumvent any school policy is prohibited. Users may not alter the settings on a computer in such a way that the virus protection software would be disabled. Users are not to try to guess passwords. Users may not simultaneously log in to more than one computer with one account. Users are not to access any secured files, resources, or administrative areas of the school network without express permission or the proper authority.

No AUP can detail all possible examples of unacceptable behavior related to technology use. Users are expected to understand that the same rules, guidelines, and policies that apply to non-technology related behavior also apply to technology-related behavior. Our school technology Users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet.

School Response to Violations of AUP

The school's network and other administrators shall have broad authority to interpret and apply the rules and guidelines contained within this AUP. Restrictions may be placed on violator's use of school technologies and privileges related to technology use may be revoked entirely pending any hearing to protect the safety and well-being of our community. School authorities have the right to confiscate personally owned technological devices that are in violation or used in violation of school policies. Violations may also be subject to discipline of other kinds within the school's discretion. Our school cooperates fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on school property or through school technologies.

If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately report this to a member of the IT department so as to demonstrate that you did not deliberately access inappropriate information.

If you witness someone else either deliberately or accidentally access inappropriate information or use technology in a way that violates this AUP, you must report the incident to a school administrator as soon as possible. Failure to do so could result in disciplinary action.

The school retains the right to suspend service, accounts, and access to data, including user files and any other stored data, without notice to the user if it is deemed that a threat exists to the integrity of the school network or other safety concern of the school.

School Liability

The school cannot and does not guarantee that the functions and services provided by and through our technology will be problem free. The school is not responsible for any damages Users may suffer, including but not limited to, loss of data or interruptions of service. The school is not responsible for the accuracy or the quality of the information obtained through school technologies. Although the school filters content obtained through school technologies, the school is not responsible for user's exposure to inappropriate information nor is the school responsible for misinformation. The school is not responsible for financial obligations arising through the use of school technologies.

General Safety and Security Tips for the Use of Technology

Posting Online and Social Networking: Never post personal information about yourself online. Personal information includes your phone number, address, full name, siblings' names, and parents' names. When creating an account on a social networking Web site, make sure to set your privacy settings so only your friends can view your pictures and your profile. Avoid accepting a friend you do not already know. If possible, set up your account so that you are notified of any postings onto your wall or page. If possible, set up your account so that you have to approve all postings to your wall or page. If possible, set up your account to notify you when someone else has posted and tagged you in a picture. If you have a public profile, be careful about posting anything identifiable such as a sports team number or local park where you spend your free time.

Communications: Think before you send all forms of communication, including e-mails, IM's, and text messages. Once you send the data it is not retrievable, and those who receive it may make it public or send it along to others, despite your intentions.

Strangers: Do not feel bad about ignoring instant messages or e-mails from unknown people. Save all contacts from known or unknown people who are repeatedly contacting or harassing you. These saved messages will help authorities track, locate, and prosecute cyber-stalkers and cyber-bullies. If you have been speaking with a stranger online and make plans to meet the stranger in person, notify your parents or guardians first.

Passwords: Do not share your passwords with your friends. When creating a password, do not make it anything obvious such as your pet's name or favorite sports team. Also remember to include both letters and numbers in your password if possible.

Downloads and Attachments: Do not open or run files, or click on links in e-mails, on your computer from unknown or suspect senders and sources. Many viruses and other undesirable consequences can result from opening these items.

Stay Current: Do protect your own computer and devices by keeping antivirus and antispyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.

Termination of Accounts and Access

Upon graduation or other termination of your official status at our institution, you will no longer have access to the school network, files stored on the school network, or your school-provided e-mail account. Prior to departure, we recommend that you save all personal data stored on school technology to a removable hard drive and set up an alternative e-mail account. If you leave our institution in good standing, we will continue to provide e-mail account access for a period of 60 days after your departure date. Otherwise, access to all technology resources is terminated immediately.

Right to Update

Since technology is continually evolving, our school reserves the right to change, update, and edit its technology policies at any time in order to continually protect the safety and well-being of our Users and community. To this end, the school may add additional rules, restrictions, and guidelines at any time.

Please print student name **(Required)**

For students: I have read the Wilbraham & Monson Academy Acceptable Use of Technology Policy, and I agree to abide by its conditions.

Student signature

Date

For parents: I have read the Wilbraham & Monson Academy Acceptable Use of Technology Policy, and I agree to the terms of the AUP as it relates to my son or daughter's usage of the technology provided by WMA.

Parent/guardian signature

Date

The student signatures are required at registration. You may download this signature page, sign and date it, and bring it to registration. If you will not be accompanying your son/daughter to registration, you may download and sign the page and fax or mail it to the Academy to the attention of the Deans Office by September 21. It is important that you return this page to the Deans Office by that deadline.

The Wilbraham & Monson Academy Acceptable Use of Technology Policy can be found on the Academy Web site at www.WMA.us/AUP.