Wilbraham & Monson Academy

ACCEPTABLE USE OF TECHNOLOGY POLICY

2019-2020

ACCEPTABLE USE POLICY

A. INTRODUCTION AND OVERVIEW

Access to information technologies is integral to the educational mission and purpose of Wilbraham & Monson Academy (WMA or the "School"). We utilize technology in nearly every facet of instruction, activity, service, research and operation of our School. This Acceptable Use of Technology Policy ("AUTP") 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 complement 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.

B. SCOPE AND ACKNOWLEDGMENT

This AUTP applies to all students, all faculty and staff members and all visitors to campus (both adults and minors) including parents and independent sub-contractors, hereinafter ("Users").

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

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

C. USE OF SCHOOL'S NAME AND IMAGE

Our School 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 website 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 website profile or a website that involves rating or judging of another member of the WMA community.

D. 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.

E. 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.

F. 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 their parent/guardian if they are 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 things, 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.

G. 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 or by a member of a school staff including, but not limited to, an educator, administrator, school nurse, cafeteria worker, custodian, bus driver, athletic coach, advisor to an extracurricular activity or paraprofessional 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 cyberbullying. (M.G.L. c. 71, § 37O)

Cyberbullying – Cyberbullying 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. Cyberbullying shall also include (i) the creation of a webpage 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. Cyberbullying 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 or on the School's network. 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, wireless access points, 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 AUTP, 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.

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, CDs, DVDs, calculators, scanners, printers, cameras, external and/or portable hard drives, Ethernet cables, servers, Wi-Fi hot spots, routers and the internet. School technology refers to all technology owned and/or operated by the School.

User – For the purposes of this AUTP, 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.

H. 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 emails 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 AUTP, 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 emails and other data for their child's technology account at the 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.

I. 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.

1. 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 email account. All emails 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. Email 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.

The School has wired Ethernet ports as well as wireless network access that is protected by a password. Unauthorized access is forbidden, which includes providing your access or wireless password 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.

J. 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.

K. 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 and software.

1. 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	Every day: 5 a.m. – 2 a.m.
Juniors/Sophomores	Sunday-Thursday: 5 a.m. – 10:45 p.m. Friday: 5 a.m. – 11 p.m. Saturday: 5 a.m. – 11:30 p.m.
Freshmen	Every day: 5 a.m. – 10:45 p.m.
Middle School students	Every day: 5 a.m. – 9 p.m.

2. ACTIVITY

Examples of allowable recreational uses of School technology resources include:

- non-school related research
- playing appropriate and non-offensive online games
- communicating with friends and/or family members
- updating profiles or accounts on social networking websites
- looking at pictures or watching YouTube videos
- similar activities that do not otherwise violate School policy

3. 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 a student consistently uses an excessive amount of data, the School reserves the right to remove their access to the internet.

4. DOWNLOADS AND FILE SHARING

Users may never download, add or install new programs, software or hardware onto School-owned computers. If material is needed for specific academic projects, please contact the helpdesk in advance for assistance. 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.

5. GAMING DEVICES

Users may play appropriate and non-offensive PC and console video games using the School's technology resources. If a User has been identified as using a large amount of the School's bandwidth or network resources to play a video game, the User may be asked to delay their game if someone else needs the bandwidth to complete school work. Repeated warnings of bandwidth overuse will result in suspension of privileges. Academics have priority over computer gaming. Please refrain from using School computers for gaming.

6. PROHIBITED DEVICES

Students may not install or use their own wireless routers or access points in the dorms or around campus. These devices can interfere with WMA Wi-Fi routers/access points, network switches, Smart TVs and cause slow Wi-Fi for everyone. Network hubs and switches in dorm rooms are also not supported.

L. PERSONAL ELECTRONIC DEVICES

Technology can enhance the learning experience, and these procedures assist us in creating healthy and safe practices for our community. Focusing on safety, community members are not allowed to use e-devices while crossing the street, walking down stairs or passing through doorways, with the possible exception of a phone call.

Cell phones, smartphones, translators, laptops, tablets and other e-devices may not be turned on, used for any reason, or visible during any academic classes, afternoon activity meetings or competitions, school meetings, study hall or any other school commitment or obligation, unless permission is specifically granted by the adult leaders of the activity for the purposes of the program. E-devices may be used for relevant class work when specifically permitted by the faculty. Upper School faculty also have storage units in classrooms for cell phones and can require students to turn off their e-devices and place them in these storage containers. Middle school students will store their cell phones in the MS office during the academic day. If parents need to contact their child, they can call the MS administrative assistant, who will coordinate the communication.

Any student utilizing an unauthorized electronic device during an academic assessment will be sent to the Deans Office immediately under the automatic assumption of academic dishonesty and standard academic and disciplinary consequences will apply.

Headphones, earbuds or other personal audio listening implements are only allowed in personal areas, such as dorm rooms, or when academic endeavors warrant their use and the teacher grants permission. If permitted in class or during study hall, the volume must remain at a level that teachers' instructions can still be heard. Otherwise, such devices block hearing and prohibit social interaction, which is antithetical to being a member of an interactive community, and they are therefore not allowed. Playing music and videos out loud should be kept to personal areas, such as dorm rooms, and not in public spaces or hallways. Using e-devices in the dining hall is limited to specifically reserved tables. The rest of the tables in the dining hall are community tables, and using devices at them is not allowed. If community members must take an emergency call, they must excuse themselves and go to the dining hall lobby to use the phone.

Inappropriate use of personal electronic devices, which includes, but is not limited to bullying, harassing and sexting, may result in disciplinary action. "Sexting" means sending a sexually explicit or sexually suggestive photo or video over an electronic device. It is a crime to create, send or possess sexually explicit photos or videos of a minor (even if the photo is of you, or if it is sent to your partner). Therefore, students are not allowed to transmit, possess or display for others any such inappropriate photos or videos on their electronic devices. If any student is participating in this in any way, they may face school discipline and/or police action.

If a student violates any of these rules, the associated electronic device will be confiscated by the discovering faculty member and turned in to the Deans Office.

M. 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. Capturing others in the WMA community on such devices (video, photo, audio or otherwise) is prohibited without the consent and intended use agreed upon by all parties. Google Glasses or any anonymous video capturing devices are strictly prohibited from campus.

N. SOCIAL NETWORKING AND WEBSITE USAGE

Members of the community may access their profiles or accounts on social networking websites 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 website from a School-owned computer and another User needs the computer for academic purposes.

Users may access their own pictures or view pictures of others on photography sharing social media, but they may be asked to give up the computer if they are accessing a photography sharing website from a School-owned computer for non-academic reasons and another User needs the computer for schoolwork.

Users are not permitted to access from the School's technology any websites 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' current WMA students, or otherwise establish a direct social link with WMA students on social networking sites.

O. COMMUNICATION: INSTANT MESSAGING, EMAIL, 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 cyberbullying and will not be tolerated. Any cyberbullying, 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 emails, instant messages or text messages.

P. 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 AUTP.

Users who are engaged in fundraising campaigns for School-sponsored events and causes must seek permission from the Deans Office before using technology resources to solicit funds for their event.

Q. 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 resetting 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 websites or VPN’s to tunnel around firewalls and filtering software is expressly prohibited. The use of websites to anonymize the User is also prohibited. The use of websites, 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 AUTP 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.

R. ACADEMY'S 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 AUTP. 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 AUTP, 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.

S. 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 the

School technologies. Although the School filters content obtained through School technologies, 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.

T. GENERAL SAFETY AND SECURITY TIPS FOR THE USE OF TECHNOLOGY

1. 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 website, 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.

2. COMMUNICATIONS

Think before you send all forms of communication, including emails, 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.

3. STRANGERS

Do not feel bad about ignoring instant messages or emails 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 cyberstalkers and cyberbullies. If you have been speaking with a stranger online and make plans to meet the stranger in person, notify your parents or guardians first.

4. 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.

5. DOWNLOADS AND ATTACHMENTS

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

6. STAY CURRENT

Do protect your own computer and devices by keeping anti-virus and anti-spyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.

U. TERMINATION OF ACCOUNTS AND ACCESS

Upon graduation or other termination of your official status at our School, you will no longer have access to the School network, files stored on the School network or your School-provided email 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 email account. If you leave our School in good standing, we will continue to provide email account access for a period of 30 days after your departure date. Otherwise, access to all technology resources is terminated immediately.

V. RIGHT TO UPDATE

Since technology is continually evolving, our School reserves the rights 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.