Houston Academy's Technology
Acceptable Use Policy

2021–2022

Houston Academy is committed to Student use of technology as a tool to expand learning opportunities and conduct scholarly research. The use of technology facilitates global collaboration, which is a vital skill for 21st century learners. Students at Houston Academy utilize laptop computers on a wireless network. Laptops and campus computers are strictly for educational use consistent with the educational goals of Houston Academy. Responsibility accompanies this opportunity. This Acceptable Use Policy (AUP) is designed to give Students and their families clear and concise guidelines regarding the appropriate use of technology, both of these laptops and other electronic devices, such as cell phones. The underlying premise of this Policy is that all members of the Houston Academy community must uphold the values of honesty and integrity. The proper use of technology reflects the strength of one's character, as does one's behavior. We expect our Students to exercise good judgment and to utilize technology with integrity.

Inappropriate Content and Use
- Inappropriate materials are available on the Internet and are strictly prohibited. These materials include items of a sexual or pornographic nature, extremist or militant materials, gambling, depictions of violence, images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.
- If a Student accidentally accesses a website that contains obscene, pornographic, or otherwise offensive material, he/she is to notify a teacher or a member of the Technology Department as quickly as possible, so that such sites can be blocked from further access. This is not merely a request; it is a requirement.
- Screensavers may not contain copyrighted media or inappropriate content, including the presence of weapons, pornographic materials, inappropriate language, alcohol, drugs, or gang-related images.
- Students may not use their laptop or any other electronic device to create inappropriate content of any kind.
- Use of electronic devices to cheat in any form is strictly prohibited. Cheating includes, but is not limited to, gaining information through electronic means without teacher approval.

Cyber-bullying
- Cyber-bullying is defined as bullying through the use of technology or any electronic communication, which includes but is not limited to any transfer of signs, signals, writing, images, sounds, videos, or data of any nature, transmitted in whole or in part by such things as instant message, e-mail, or text message, using any electronic device, including, but not limited to computers and cell phones.
- Cyber-bullying also includes the creation of a social networking account, a web page, or a blog in which the creator assumes the identity of another.
- Cyber-bullying is strictly prohibited and is subject to appropriate consequences including prosecution. This applies whether the cyber-bullying occurs on or off our school campus.

E-Mail
- Students are prohibited from using an email account during school hours other than their school-issued account.
- No inappropriate e-mail may be sent that contains derogatory, obscene, or harassing language or images. Such messages will be regarded as a major infraction and will be subject to a disciplinary response.
- Spam and chain letters of any kind are prohibited. Chain letters are defined as any e-mail message asking you to pass information or messages on to other individuals or groups via e-mail. Students should attempt to refrain from opening such e-mails.
- Students are prohibited from accessing anyone else's e-mail account.

Social Networking
- Instant messaging, blogging, and participating in chat rooms are prohibited on campus except as part of an assigned, in-class activity that is supervised by faculty or administration.
- Use of social networking sites, including but not limited to, Snapchat, Instagram, TikTok, Pinterest, Twitter, and Vimeo, is prohibited during school hours.

Audio and Video
- Audio on electronic devices should be turned off during class time unless required for an assigned activity. When sound is needed, the Student must use headphones he/she has provided.
- Listening to music either aloud or with earphones is permitted during class or study hall only at the discretion of the teacher. Listening to music during free period or other times while on campus is permissible unless it is disruptive to the activities taking place. Faculty and staff can restrict this at their discretion.
- The use of electronic devices to watch movies or videos, unless assigned by a teacher, is not permitted during the school day.
- Any audio or video recording is prohibited without the permission of all parties being recorded. This applies to audio or video recorded through the use of any electronic device, including, but not limited to, computers or cell phones.
- No written, audio, or video account of any activities taking place on the campus of Houston Academy or during any school sponsored activity or trip shall be posted to the Internet without the expressed permission of a faculty member.
- Illegal sharing or viewing of copyrighted music or movies is strictly prohibited and is subject to appropriate consequences including prosecution.

Games
- The viewing and/or playing of electronic games on any electronic device is not permitted on campus during school hours except as part of an assigned, in-class activity.
- Games that include violence, adult content, inappropriate language, or weapons are not to be installed or played on the laptops. The School reserves the right to remove any game from the laptop that is considered inappropriate or impedes the educational purpose of the laptop program.
- No games that are played over the School network are allowed, except as part of an Esports team practice or competition.
- Illegal sharing or viewing of copyrighted games is strictly prohibited and is subject to appropriate consequences including prosecution.

Laptop Care

- Student laptops must not be left unattended at any time. If a laptop is found to be unattended, it must be turned in to the Dean of Students. Laptops must be in a Student's possession or secured in a locked classroom or locker at all times.
- Do not lend your laptop to other students or any third party.
- Do not borrow a laptop from another student.
- Laptops must be carried and transported in an approved computer messenger bag at all times. **Backpacks, even with a padded pocket, are not to be used as laptop bags.** Note: Students are entirely responsible for backing up their own data. Lost or damaged data is not the responsibility of the School.
- No food or beverages should be in the vicinity of the laptops. Laptops may not be used in an area where food or drink is present during break, lunch, or at any other time.
- Laptops should be handled with respect and care. Inappropriate treatment of School laptops is not acceptable.
- Laptops are not to be written on, have stickers applied to them, or be defaced in any way.
- Do not remove, move, or write on the identification sticker on your laptop.
- All computer messenger bags must have an identifying luggage tag.

Network Access – The user is responsible for his/her actions and activities involving the network. Some examples of unacceptable uses include, but are not limited to, the following:
- Hacking or gaining unauthorized access to systems, servers, files, resources, or entities.
- Avoiding the use of our School filtering software to access the Internet from school or home.
- Using the network for entering contests, advertising, political lobbying, or personal commercial activities, including online selling or purchasing.
- Using another person's password or knowingly giving one's password to others.
- Printing non-school related materials on School printers.
- Using terminal services to access or modify remote systems.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal law. This includes tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.

File Sharing-File sharing is the public or private sharing of computer data or space. Any program that creates a point-to-point connection between two or more computing devices for the purpose of sharing data is also considered file sharing.
- File sharing of any kind is prohibited both on campus and off campus. This includes, but is not limited to, the sharing or copying of work between Students and the plagiarizing of any work. The only exception to Students sharing work is when an assignment given by a faculty member requires the Student to collaborate.
- No file sharing software of any kind is to be installed on School laptops.

Deleting Files
- Do not delete any folders or files that you did not create or that you do not recognize. Deletion of certain files will result in a computer failure, will interfere with your ability to complete class work, and may affect your grades.

Downloading and Loading of Software
- Students are not permitted to install custom/individual applications that require administrator privileges.
- All installed software must be a legally licensed copy.
- The downloading of music files, video files, games, etc. is prohibited during school hours, except as part of an assigned, in-class activity that is supervised by faculty or administration.
- The School reserves the right to remove any software that has been loaded onto the computer that impedes the educational purpose of the laptop program.
- Copyrighted movies may not be downloaded from the Internet and placed on the laptops.
- Only commercial videos legally purchased from the iTunes store or another like entity may be downloaded to the laptops.
- In no event shall any Student load, install, or view any software, images, data or other content on any School laptop that impedes the educational purpose of the School's laptop program and/or of the laptop or in any way limits the laptop's capacity to fulfill its educational purposes.

Privacy, Use, and Safety

- Students may not give any personal information regarding themselves or others through e-mail or the Internet including name, phone number, address, passwords, etc. unless they are completely sure of the identity of the person with whom they are communicating. Frequently the identity of someone on the Internet is impossible to confirm. Therefore, contact with such individuals is considered inappropriate and unsafe.
- Students are not to provide the e-mail address or other personal information regarding other Students, faculty, or administration to anyone outside of the school without their permission.
- Students must secure and maintain private passwords for network and laptop access. This is important in order to protect the privacy of each Student. Do NOT share personal passwords or usernames.
- Houston Academy respects the privacy of every Student, faculty member, and administrator with respect to stored files and e-mail accounts. However, for any reason in the sole discretion of Houston Academy, its faculty, administration, and the Director of Technology, including but not limited to suspicion of inappropriate use, honor code violations or harassment, the School's administration has the right to view or remove any of the content on each Student's laptop at any time.
- The School will monitor computer activities that take place on School-owned computers including logging website access, newsgroup access, bandwidth, and network use.
- Students are not allowed to create any administrative passwords on their laptops.
- Students are prohibited from accessing faculty, administration, and staff computers for any reason without explicit permission from the user or administrator of that computer.
- Students are prohibited from utilizing the command prompt interface. In addition to this limitation, Students are prohibited from using any method to obtain control of another person's computer through the use of their own computer.
- Laptops that are provided by the School continue to be the property of the School. The School network is a closed, secured network. If at any time, privately owned devices are allowed on the School network, they are subject to all policies and consequences of this Acceptable Use Policy including: the right to view the content of the device at any time; the right to remove content from the device; and the right to retain the device in the School's possession if there is an infraction to the AUP that deserves that consequence.

Consequences

- The School reserves the right to enforce appropriate consequences for the violation of any section of this Acceptable Use Policy. Violations will be considered minor or major infractions of our discipline policy, depending on the severity of the violation. Consequences of violations include the loss of privileges on a laptop, the loss of the use of any computer for an amount of time determined by the administration, other disciplinary action up to and including expulsion, and possible legal action.
- Computers with illegal or inappropriate software or materials on them will be reformatted or "re-imaged," and **the Student will be charged a $25 AUP violation fee PER incident for this service. This amount may be increased for repeat violations.**
- In the case of repeated laptop abuse and/or damages, the School has the right to revoke the use of the School's laptop and the Student will be restricted to using only on-campus computers. Repeated AUP offenses or laptop abuses may lead to the loss of the Student's privilege of using any computer on campus.
- Students are to report any known violations of this Acceptable Use Policy to the faculty, administration, or Director of Technology of the School. This is not merely a request; it is a requirement. Random checks of Student laptops will be conducted throughout the year to ensure that these policies are being followed.
- Houston Academy accepts no responsibility for activities conducted on School computers and laptops or materials stored on computers, laptops, or the School's network.