Technology
Acceptable Use Policy (AUP)
Student Edition

Revised July 2021

I. Introduction and Overview

Access to information technology is integral to the educational mission and purpose of our institution. We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our school. This policy provides expectations for the use of technology as it affects our school and educational community.

Due to the evolutionary nature of technology, it is imperative for students to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all students 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. Students should be sure to read and understand the policies below before using the School's network and other technologies, as well as any personally-owned technology. Use of school technology resources will imply understanding and agreement to the terms set forth in this policy. These policies apply to all students regardless of classes being in or out of session.**

Right to Update this Acceptable Use Policy

Because technology, and our intended use of technology are continually evolving, our school reserves the right to change, update, and edit its technology policies at any time in order to meet procedural and instructional needs, while protecting the safety and well-being of our students and community. To this end, the Academy may add additional rules, restrictions, and guidelines at any time.

Supervision and Personal Responsibility

This policy applies only to students. All children and teens visiting our campus are also subject to the terms and conditions of this Technology Acceptable Use Policy. Students and parents are required to read this Acceptable Use Policy and signify compliance annually by signing the school's Student Handbook.

> **Junior and Country Day School** students will be supervised by teachers at all times and will only use technology under the supervision of a teacher.
>
> **Middle School** students are expected to be responsible in their technology and Internet use at such a level that they may use these devices without direct supervision.
>
> **Senior School** students are expected to be responsible in their technology and Internet use at such a level that they may use these devices without direct supervision.

Technology as a Privilege

The use of school-owned technology devices and networks, on school property or at school events, is a privilege not a right. This privilege comes with personal responsibility; and if a student fails to act responsibly with their use of technology, the privilege of that use may be suspended and/or revoked.

Our school provides sufficient technology resources for each student for regular academic pursuits. If a particular research project requires additional access or resources, the Information Technology Department will work with teachers and school administrators and make a best effort to provide for those additional needs.

Privacy
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. All on-campus web browsing may be monitored. Any files saved onto school-owned technology, or under school-based accounts can also be inspected. Students should have a limited expectation of privacy when using their own technology on school property or at school events. The Academy will usually not interfere with student technology use, as long as no activity violates policy, law and/or compromises the safety and well-being of the school community.

Filtering
The 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.

Termination of Accounts and Access
Upon graduation from Shady Side Academy, students will be permitted access to their school email account for 90 days. Prior to graduation, it is recommended that students save personal data stored on school technology or under school-based accounts to a removable storage device and setup an alternate email account. Any student who leaves Shady Side Academy before the end of the school year for any reason will have his or her email account closed on his or her last day.

II. Definitions and Terms

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

Cyber-Bullying
Cyber-bullying is when someone sends derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyber-bullying also takes place when someone purposefully excludes someone else online. For example, a group of students create a group on a social media platform that many would like to join, but the student creators purposefully exclude one individual or certain individuals and do not let them join their group. Cyber-bullying also takes place when someone creates a fake account or website impersonating, criticizing or making fun of another.

Network
The network is defined as the school's computers, mobile devices, and other digital electronic equipment (such as printers/copiers, interactive whiteboards, projectors, etc.), and the wired and/or wireless communications network on which they operate.

User
For the purposes of this policy, user is an inclusive term meaning anyone who utilizes or attempts to utilize technology owned by the school. This includes students, faculty members, staff members, parents, and any visitors to the campus.

Mobile Device
For purposes of this policy, a Mobile Device is any portable electronic device which provides some of the functions of a computer, a cell phone, a music player, and a camera.

III. Acceptable and Unacceptable Uses of Technology

Purposes and Use Expectations for Technology
All school-owned technologies, the school network, and its Internet connection are intended primarily for educational purposes. Educational purposes include academic research and collaboration, classroom activities, career development, communication with experts, homework, and a variety of other activities. Many recreational uses of the school network and other technologies are permitted, unless those activities are prohibited elsewhere in this policy, or in cases where the activity interferes with any educational or operational process of the school, teachers or other students. In any case where a teacher or other school employee directs a student to cease a given activity, the student should comply. The school is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology.

Senior School students in the boarding program may use school technology for more broad recreational purposes in the dorms, and outside of school hours only. Acceptable boarding-student recreational uses of technology include:

- Playing appropriate and non-offensive games
- Communicating with friends and/or family members
- Using voice over Internet technologies
- Updating profiles or accounts on social networking websites
- Engaging in other activities that do not otherwise violate school policy

If a student's recreational use of shared technology resources should interfere with another user's educational needs, that student may be asked to stop those activities.

Both wired and wireless connectivity is provided across all campuses, including in the Senior School dorms. The Academy's data network is to be used by students for connecting end-user devices only, not additional networking equipment. Students may not attempt to extend the Academy's network by attaching personal routers, switches, or other network equipment.

Personal Responsibility
We expect our students to act responsibly and thoughtfully when it comes to using technology. Technology is a finite shared resource offered by the school to its students. Students 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.

School-Provided Technology Resources
All students are provided with a school email account, which is introduced to students at an age-appropriate time, and when instructional practices require email correspondence. All emails sent from this account are representative of the School, and students should keep in mind school policies regarding appropriate language use, bullying, stalking, and other policies and laws. Student email accounts are subject to monitoring and have limited privacy.

The School provides individual technology accounts for students. Students must log off when they are finished using a school computer, or another user may access their account, files, and email. Actions that take place under a given user account are accountable to the owner of that account. Users should keep network passwords private and should never deliberately share network account information with another student.

International Websites
Since many foreign language websites cannot be accurately read by the School's automated content filtering systems, these websites may not be accurately categorized or filtered, usually erring on the side of blocking unrecognized content. If access to an International website is required for study, a request may be made to the Technology Department, through the teacher requiring the school work or study.

Cell Phones, Portable Game Devices, and other Mobile Devices
Mobile apps such as calculator, camera, voice-recorder, and an unlimited number of other communications and collaborative apps available on many smart phones may have educational relevance, and may be utilized in a responsible manner if the supervising teacher or adult permits. Please refer to each division's *Student Handbook* for more information dealing with cell phone and mobile device use by students.

> **Junior and Country Day School** students are not permitted to have cell phones, smart watches, or other personal electronic devices during the school day. If there is a need for a student to make a phone call, telephones are available in the Junior and Country Day School offices. Phones, smart watches, and other devices must be turned off and left in backpacks or lockers throughout the school day. If used during the school day, such devices will be confiscated.
>
> **Middle School** students are permitted to have cell phones in the building, but those phones must be kept in student lockers during the school day unless otherwise permitted by an individual teacher.
>
> **Senior School** students may carry cell phones on campus. Cell phones may be used during academic hours for non-verbal communication only. Cell phones may be allowed in classroom settings, per individual teacher and/or departmental policy. Please refer to the Senior School Student Handbook for the complete cell phone policy.

Recording, Video, and Photography
Students are only permitted to capture or send photographs, video or live streaming content on school property or at school events under the supervision of a teacher. Any student appearing in captured photos or video may not be identified by name. Furthermore, students may not capture personally identifiable audio, photos, or video footage without documented permission from those being recorded.

Social Networking, Photo-Sharing, Instant Messaging, and Web Publishing Technologies
Access to social networking websites, photo-sharing websites, messaging tools, and online publishing such as blogging and website creation tools will be controlled by Internet filtering technology. However, based on grade-level appropriateness, and instructional relevance, certain identified social networking sites may be permitted. Therefore, students may have profiles and/or accounts on these types of sites, and may utilize these tools, and digital social connections for responsible academic collaboration and sharing. Other use of these types of tools and websites shall be subject to the terms set forth in this Acceptable Use Policy.

Students may not access from the school's technology any online dating websites or rating sites such as, but not limited to, Match.com, Tinder, RateMyTeacher.com, RateMyCoach.com, or JuicyCampus.com.

Inappropriate Material
Students 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).

Inappropriate Communications
Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students. 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 students; 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 a student is asked by another person to stop sending communications, the student must stop.

Students may not engage in any form of cyber-bullying, i.e., using any technology to harass, insult, antagonize, slander, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. Cyber-bullying in any form is unacceptable and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of a person or the school is subject to disciplinary action.

Students may 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.

Intellectual Property, Academic Honesty, Personal Integrity and Plagiarism
Plagiarism – *claiming or implying that someone else's work, image, text, music, or video is a student's own, or incorporating portions of someone else's works into a student's own work without citing* – is unacceptable and will not be tolerated. All students are expected to maintain academic honesty. Students may 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. A student should not post or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than him/herself. This includes intellectual property that students were given permission to use personally, but not publicly. This behavior violates school policy as well as state and Federal laws.

A work or item is copyrighted when 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 the copying or reproducing of copyrighted material without the authority to do so. Students must make sure to appropriately cite all resources used in all work. Students should never utilize someone else's work without proper permission.

Downloads and File Sharing
Downloaded media files should not be stored on school-provided local or cloud storage. Students may never download, add, or install new programs, software, or hardware onto school-owned computers, unless expressly directed by a teacher and permitted by the IT Department. Students may never configure a school computer or personally owned computer to transmit or receive copyrighted material, or to engage in any illegal file sharing. The 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.

Commercial Use
Commercial use of school technology is prohibited. Students may not use school technology to sell, purchase, or barter any products or services. Students may not resell school-supplied network resources to others, including, but not limited to, network/Internet access, and disk storage space. The School is not

responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology.

- *At the Senior School, students engaged in fund-raising campaigns for school-sponsored events and causes must seek permission from the Deans' Office before using technology resources to solicit funds for the event.*

Political Use
Political use of school technology is prohibited without prior, specific permission from the Head of School. Students may not use school technology to campaign for/against, fundraise for, endorse, support, criticize or otherwise be involved with political candidates, campaigns or causes.

Respect for the Privacy of Others and Personal Safety
Our school is a community. Community members must respect the privacy of others.

- Students may not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others.
- Students may not misrepresent or falsely assume the identity of others.
- Students may not re-post information that was received privately without the permission of the sender/owner of the information.
- Students may not post private information about others.
- Students may not use another person's account.
- In circumstances where a student has been given another user's account with special privileges, that account may not be used outside of the terms under which it was given.

Students may not voluntarily post private/personal information online, including name, age, school name, address, phone number, or other identifying information.

Respect for Shady Side Academy and the SSA Community
Shady Side Academy takes pride itself in its reputation for excellence; therefore, no person/organization, including students may 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 Academy's name, emblem, or logo. This also includes listing the school's name or school employees on social networking platforms, dating websites, or a rating website such as RateMyTeacher.com or RateMyCoach.com.

Computer Settings and Student Behaviors
All school technology users are expected to understand that the same rules, guidelines, and policies that apply to other student behavior also apply to technology-related student behavior. Students are expected to use their best judgment when making decisions regarding the use of all technology and the Internet. While no policy could detail all possible examples of unacceptable behavior related to technology use, here is a brief list highlighting some examples experienced within our schools:

- Students may not eat or drink while using any school-owned computers or other technologies.
- Students may not alter, change, modify, repair, or reconfigure settings on school-owned computers without the express prior permission of school technology staff.
- Students may not purposefully spread or facilitate the spread of a computer virus or other harmful computer program, or alter settings on school-owned technology in such a way that the virus protection software or other security measures would be disabled.
- Students may not take action to circumvent any school-applied system security measures.
- Students may not use domestic or international websites to tunnel around firewalls and Internet content filtering software, or to hide their identity when browsing.

- Students may not use websites or other software utilities to circumvent any security meant to ensure compliance with this policy and state and/or Federal law.
- Students may not attempt to guess passwords or utilize any password hacking utilities to acquire passwords. Students may not log in to more than one computer with the same account at the same time.
- Students are not to access any secured files, resources, or administrative areas of the school network without express permission or the proper authority.

IV. Responses to Violation of the Responsible Computing Policy

The school's Director of Educational Technology, Network Administrator, and other school administrators shall have broad authority to interpret and apply these policies. Violators of the Academy's technology policies will be notified and given the opportunity to explain their actions in the manner set forth in each division's *Student Handbook*, unless an issue is so severe that notice is neither possible nor prudent in the determination of the school administrators. Restrictions may be placed on the violator's use of school technologies. Depending on the nature of the action, and to protect the safety and well-being of our community, technology privileges may be revoked entirely pending any hearing. Violations may also be subject to discipline of other kinds within the school's discretion. The 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. School authorities have the right to confiscate personally-owned technology devices that are in violation or used in violation of school policies.

Students in receipt of, or gaining access to inappropriate information, even accidentally, should immediately inform a teacher or school administrator. Failure to do so may place responsibility for the inappropriate content on the student. Any student to witness another, either deliberately or accidentally access inappropriate information or use technology in a way that violates this policy should 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 disable network user accounts, and/or suspend access to data, including student files and any other stored data, without notice to the student if it is deemed that a threat to school safety or to the integrity of the school network exists.

V. 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 students 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 Internet and email content, the school is not responsible for a student's exposure to "unacceptable" information, nor is the School responsible for misinformation. The school will not be responsible for financial obligations arising from student use of school technologies.

VI. General Safety and Security Tips for the Use of Technology

Posting Online and Social Networking
Students should never post private/personal information online. Personal information includes phone number, address, full name, siblings' names, and parents' names. When creating an account on a social networking website, make sure to set privacy settings so only friends can view pictures and profile information. Students should avoid accepting "friends" not already known. Social networking accounts should be configured to notify of all photo tagging. Students should avoid posting any personally identifiable information or content to publicly available social network profiles.

Communications
All forms of electronic communication, including email and text messages are not retrievable. Those who receive these correspondence may share publicly regardless of the sender's intent.

Strangers
Students should save all repeated and/or harassing messages from both known and unknown senders. These saved messages will help authorities track, locate, and prosecute cyber-stalkers and cyber-bullies. Students should never arrange to meet strangers encountered online.

Passwords
As a best practice, passwords should contain both upper and lower case letters, and at least one number or other special character. Passwords should not be easily guessable, and should not be formed from personal information such as a child's or pet's name. Students should not share passwords with friends.

Downloads and Attachments
Students should not open or run electronic files from unknown or suspicious senders or websites. Harmful and undesirable consequences can result from opening these items.

Stay Current
Students should protect personal computers and other devices by keeping antivirus and antispyware, operating systems, and application software up to date. Students should disable file sharing, and other ad hoc peer-to-peer networking capabilities on personal devices.