

STUDENT COMPUTING DEVICES/EQUIPMENT POLICY AND ACCEPTABLE USE AGREEMENT

Board Policy #: SAE-BP-014

Adopted/Ratified: September 9, 2021

Revision Date: September 9, 2021

Technology resources at The School of Arts and Enterprise (“The SAE” and the “Charter School”) are provided for the purpose of supporting the mission and vision of The SAE. The goal in providing these devices is to promote educational excellence by facilitating resource sharing, innovation, research, creativity, communication, increased productivity, and mobile learning.

The SAE’s unique focus on the integration of arts and academics is considered in this policy and works as a safeguard for student use of technology and equipment.

Use of these technologies is a privilege that carries responsibility and behavioral expectations consistent with all school rules and policies, including, but not limited to those stated in The SAE Parent-Student Handbook. It is understood that members of our SAE community will use all types of computing devices and the school’s network in a responsible, ethical, and legal manner at all times.

The SAE retains sole right of ownership of computing devices and related equipment. The SAE retains the right to collect and/or inspect the computing device at any time, and to alter, add, or delete installed software or hardware.

Computing Devices and Equipment

Receiving Your Computing Device or Equipment

Parents/guardians and students must sign and return the Acceptable Use Agreement and Handbook Acknowledgement documents before their child is allowed to use SAE-issued technology and equipment, including but not limited to: labs, recording equipment, tablets and classroom laptops. In that agreement, the student and the student’s parent/guardian shall agree not to hold the Charter School or any Charter School staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They shall also agree to indemnify and hold harmless the Charter School and Charter School personnel for any damages or costs incurred.

Students, who transfer, withdraw or are expelled from The SAE during the school year, must surrender any device or equipment upon termination of enrollment.

Device/Equipment Return Fines

If a student willfully damages or fails any SAE device or technology, the student’s parents/guardians are liable for all damages caused by the student’s misconduct not to exceed ten thousand dollars (\$10,000), adjusted annually for inflation. After notifying the student’s parent or guardian in writing of the student’s alleged misconduct and affording the student due process The SAE may withhold the student’s grades, transcripts, and diploma until the damages have been paid. If the student and the student’s parent/guardian are unable to pay for the damages or to return the property, The SAE will provide a program of voluntary work for the minor in lieu of the payment of monetary damages. Upon completion of the voluntary work, the student’s grades and diploma will be released.

Maintenance of Devices and Equipment

Students are responsible for the general care of the device or equipment they have been issued by the school. Devices and/or Equipment that are broken or fail to work properly must be taken to The SAE's Information Technology (IT) Department for an evaluation of the equipment.

General Precautions

Devices and Equipment are school property and all users will follow this policy and The SAE's Acceptable Use Policy for technology;

- Cords and cables must be handled carefully to prevent damage;
- Laptops must be returned in their original working condition to the appropriate laptop cart and plugged in correctly;
- Devices and Equipment must remain free of any writing, drawing, stickers, or labels that are not the property of The SAE;
- Devices must never be left in an unsupervised area including but not limited to: unlocked cars, and campus common areas;
- Students may not use "skins" or stickers to "personalize" devices and equipment. Devices and Equipment are intended for all authorized students and personnel of The SAE.

Carrying Devices

The guidelines below should be followed:

- Carry laptops with both hands.
- Avoid placing too much pressure and/or weight (such as folders and workbooks) on the tablet screen or laptop.

Screen Care

Device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the device.
- Do not place anything near the device that could put pressure on the screen.
- Do not place anything that will press against the cover. Clean the screen with a soft, dry cloth, microfiber or anti-static cloth. No harsh cleaners that can damage the surface of the device can be used.
- Do not "bump" the device against walls, car doors, floors, etc. as it will eventually break the screen.

Passwords

Devices will be password protected. Students are prohibited from sharing their password with anyone else except their parents/guardians for their own protection. Students who use an account that is not their own may be subject to disciplinary consequences.

Screensavers/Background Photos

A standard screensaver or background will be pre-set on laptops and tablets. Backgrounds that are considered, but not limited to, inappropriate, abusive, hateful, harassing, or sexually explicit in nature cannot be used as a screensaver or background photo. Students are subject to consequences based on the nature of a modified screensaver/background.

Photos/Music

Photo/image storage on the devices will be for school projects only. Storage of student personal sound, music, games, programs, photos or downloaded images is not allowed.

- Students may not download music from iTunes or any other music-sharing site unless directed by or with the permission of a teacher.
- Music is only allowed on the device if provided by the teacher for educational use.
- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Non-educational games or applications are not allowed on the devices.

Managing Your Files and Saving Your Work

Saving Work to Google Docs, iCloud or The SAE Approved Data Storage Solution

It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Tablet and Laptop malfunctions are not an acceptable excuse for not submitting work; therefore, students should back up all work.

Software on Devices

Originally Installed Software

The SAE will synchronize the device to contain the necessary programs for school work. The software/apps originally installed by The SAE must remain on the tablet in usable condition and be easily accessible at all times.

Procedure for Reloading Software

If technical difficulties occur or illegal software (non SAE-approved) is discovered, devices will be restored from backup. The school does not accept responsibility for the loss of any software or documents deleted due to a reformat or reimage. In this event, the student can lose the privilege of device use.

Acceptable Use

The SAE's technology resources that are provided by the school are not transferable or extendible by students to people or groups outside the school and terminates when a student is no longer enrolled in the school.

This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the responsibilities named in this policy, privileges may be terminated, access to the school's technology resources may be denied, and the appropriate disciplinary action shall be applied.

Violations may result in disciplinary action up to and including suspension/expulsion for students. When applicable, law enforcement agencies may be involved.

Parent/Guardian Responsibilities

Parents/guardians are to talk to their children about values and the standards that they should follow that pertain to the use of the appropriate internet and all other digital media resources.

The SAE Responsibilities

- Provide internet and email access to students, including a SAE-issued email address.
- Provide data storage areas through Google Drive. The SAE reserves the right to review, monitor and restrict information stored on or transmitted via school-owned equipment and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of this Policy.

Students' Responsibilities

- Use computers/tablets in a responsible and ethical manner. Comply with general school rules concerning behavior and communication that apply to tablets/computer use.
- Use all technology resources in an appropriate manner so as to not damage school equipment. Damages include, but are not limited to, the loss of data resulting from delays, non-deliveries, or service interruptions caused by the student's own negligence, errors or omissions.
- Help The SAE protect their computer system/device by contacting an administrator or teacher about any security problems encountered.
- Monitor all activity on their account(s).
- Turn off and secure devices after use to protect work and information.
- Return devices to their source after use or as directed by The SAE personnel. In the event that the student is unsure of its source for any reason, the device should be returned to their teacher, an administrator, or the campus main office.
- Do not post personal identifiable information, including, but not limited to: name, address, or social security number.

Strictly Prohibited Student Activities

- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing school policy or law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials. Use of chat rooms, sites selling term papers, book reports and other forms of student work.
- Use of any messaging services (e.g., Google Chat, MSN Messenger, ICQ, AIM, IMO). Non-educational games or games not approved by a teacher.
- Use of social media outside of approved educational purposes (e.g. Facebook, Instagram, Snapchat). Please see "Social Media" section of this policy.
- Use of outside data disks or external attachments without prior approval from the administration or teacher.
- Changing or removing device settings or The SAE's loaded device management profiles (exceptions include personal settings such as font size, brightness, etc.).
- "Jailbreaking" a tablet/device or loading software that bypasses the system's original security measures or normal mode of operation.
- Spamming or sending mass or inappropriate emails.
- Gaining access to other students' accounts, files, and/or data.
- Use of the school's internet/email accounts for financial or commercial gain or for any illegal activity.
- Use of anonymous and/or false communications such as, but not limited to, MSN Messenger, Yahoo Messenger, email, etc.

- Participation in credit card fraud, electronic forgery or other forms of illegal behavior.
- Vandalism of school equipment (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components).
- Transmitting or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
- Bypassing The SAE's school web filter through a web proxy.
- Creating, sending, accessing or downloading material, which is abusive, hateful, harassing, or sexually explicit (e.g., engaging in inappropriate activity, such as but not limited to, sending threatening messages on social media or other forms of cyber-bullying⁴).

Social Media

Students of The SAE are expected to set and maintain high ethical standards in their use of social networking. Since social media reaches audiences far beyond the community, students must use social sites responsibly and be accountable for their actions. If a student sees anything of concern on a fellow SAE student's social networking page or account, he/she should immediately contact the school's administration, teachers, or another adult within the school.

- *"Think before you post."* The SAE asks students to use discretion when posting information onto the internet.
- The SAE reserves the right to request school-related images or content posted without permission to be removed.
- Do not misrepresent statements or information by using someone else's identity.
- Social media venues are public and information can be shared beyond a student's control. *Be conscious of what you post online as you will leave a long-lasting impression on many different audiences.*
- Do not post or link anything (photos, videos, web pages, audio files, forums, groups, fan pages, etc.) to social networking sites that you would not want friends, peers, parents, teachers, college admissions officers, or future employers to access. Any digital content that is created and/or posted will create a personal digital footprint that cannot be erased.
- When responding to others, remember to be respectful and avoid comments that may be hurtful. Do not use profane, obscene, or threatening language.
- Only accept invitations to share information from people you know. Utilize privacy settings to control access to the network, web pages, profile, posts, blogs, wikis, podcasts, digital media, forums, groups, fan pages, etc.
- Online stalkers and identity thieves are a real threat. Never share personal information, including, but not limited to, Social Security numbers, phone numbers, addresses, exact birth dates, and pictures with unknown parties or on unsecure sites.
- Users should keep passwords secure and never share passwords with others. *If someone tampers with your blog, email, or social networking account without you knowing about it, you could be held accountable.*
- Cyber-bullying is considered an act of harassment and is considered unlawful.

Tablet and Laptop Care

Students will be held responsible for maintaining school devices and keeping them in good working order. Batteries must be charged and ready by following the check-in/out policy at the school.

Devices that malfunction or are damaged must be reported to the teacher, administrator, or the campus main office. The school will be responsible for repairing devices that malfunction or are accidentally damaged. A device that is willfully damaged by the student will be repaired and the insurance deductible cost will be borne by the student. Repairs may take between 7 to 10 days to complete.

A device that is stolen must be reported immediately to a teacher, administrator, or the campus office.

Legal Propriety

Students must comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If a student is unsure, ask a teacher, administrator, or parent.

Plagiarism is a Violation of the School's Code of Conduct

Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the internet, such as graphics, movies, music, and text.

Use or possession of hacking software is strictly prohibited and violators will be subject to disciplinary action. Violation of applicable state or federal law may result in criminal prosecution.

Student Discipline

If a student violates any part of the above policy, he/she may be subject to disciplinary action in accordance with The Handbook policies and procedures outlined for discipline. Student discipline may vary based on the infraction.

Protecting and Storing the Device

Storing the Device

When students are not using devices, they should be stored in a tablet or laptop storage unit in the classroom or designated charging cart.

Devices Left in Unsupervised Areas

Under no circumstances should devices be left in unsupervised areas. Unsupervised areas include the school grounds and campus, eating areas, technology labs, unlocked classrooms, and hallways. Any device left in these areas is in danger of being stolen. If a device is found in an unsupervised area, it will be taken to the school main office.

Technology and Internet Safety

Internet Safety

In compliance with the Children's Internet Protection Act ("CIPA"), The SAE will implement filtering and/or blocking software to restrict access to Internet sites that have no educational purpose and/or contain child pornography, obscene depictions, or other materials harmful to minors under 18 years of age. The software will work by scanning for objectionable words or concepts, as determined by The SAE. However, no software is foolproof, and there is still a risk an internet user may be exposed to a site containing such materials. A user who accidentally connects to such a site must immediately disconnect from the site and notify a teacher or administrator. If a user sees another user is accessing inappropriate

sites, he/she should notify a teacher or administrator immediately. Neither the SAE nor its staff shall be responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes, misuse or negligence.

The SAE will implement a mechanism to monitor all minors' online activities, including website browsing, email use, chat room participation and other forms of electronic communications. Such a mechanism may lead to a discovery that a user has violated or may be violating this policy, the disciplinary code or the law. Monitoring is aimed to protect minors from accessing inappropriate matter, as well as help enforce this policy, on the internet. The SAE reserves the right to monitor other users' online activities, and to access review, copy, store or delete any electronic communications or files and disclose them to other school officials and/or law enforcement as it deems necessary.

The Executive Director or designees shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, maintaining the student's online reputation and ensuring their personal safety by keeping their personal information private, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats,

behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying. Students are expected to follow safe practices when using Charter School technology.

Students shall not use the Internet to perform any illegal act or to help others perform illegal acts. Illegal acts include, but are not limited to, any activities in violation of local, state, and federal law and/or accessing information designed to further criminal or dangerous activities. Such information includes, but is not limited to, information that if acted upon could cause damage, present a danger, or cause disruption to the Charter School, other students, or the community. Damaging, debilitating or disabling computers, computer networks or systems through the intentional or overuse of electronic distribution or the spreading of computer viruses or other harmful programs shall be prohibited. Any unauthorized online access to other computers by means of hacking into other computers, downloading hacker tools such as port scanners and password crackers designed to evade restrictions shall also be strictly prohibited.

If a student under the age of 18 accesses their The SAE school account or the internet outside of school, a parent/guardian must supervise the student's use of the account or Internet at all times and is completely responsible for monitoring the use. Filtering and/or blocking software may or may not be employed to screen home access to the internet. Parents/guardians should inquire at the school if they desire more detailed information about the software.

Student information shall not be posted unless it is necessary to receive information for instructional purposes, and only if the student's teacher and parent or guardian has granted permission.

Users shall not reveal on the Internet personal information about themselves or about other persons. For example, users should not reveal their full names, home addresses, telephone numbers, school addresses, or parents' names on the Internet.

Users shall not meet in person anyone they have met on the Internet in a secluded place or a private setting. Users who are under the age of 18 shall not meet in person anyone they have met on the Internet without their parent's permission.

In compliance with the Children's Online Privacy Protection Act ("COPPA"), The SAE strictly follows the rules and regulations set forth by the Federal Trade Commission and for this reason, The SAE emails

provided to students under the age of 13 are prohibited from sending and receiving emails outside of The SAE domain.

All users will abide by The SAE's security policies.

No Expectation of Privacy

The SAE System Administrator has the authority to monitor all accounts, including e-mail and other materials transmitted or received via the accounts. All such materials are the property of The SAE. Account users do not have any right to or expectation of privacy regarding such materials.

Penalties for Improper Use of The SAE Accounts

The use of the account is a privilege, not a right, and inappropriate use will result in the restriction or cancellation of the account. Inappropriate use may lead to any disciplinary and/or legal action, including but not limited to suspension or expulsion, or criminal prosecution by government authorities. The SAE will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

Computer and Internet Policies

Computers are available for students' academic use in classrooms and in the Main Campus computer lab, Middle School computer lab, and the DTC Campus computer lab.

While The SAE attempts to provide complete computer and internet access to its students, computer facilities are limited. The SAE upholds community standards of decency in computer use and students will lose computer privileges should they engage in any conduct that violates this Policy or other SAE policies.

Computers in classrooms are managed by the classroom teachers and cannot be used without their permission.

The computer labs are available to students during regular school hours when classroom teachers have arranged for its use and/or if classroom teachers have made specific arrangements with the Digital Media Faculty. Before and after school, as well as during lunch, use of the computer lab is a privilege that can be given or taken away at the discretion of school faculty and staff.

Notice

All employees shall receive a copy of this policy and the accompanying Acceptable Use Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All employees shall comply with this policy and the Acceptable Use Agreement, in addition to any separate policies governing employee use of technology. Student use of Charter School's computers, networks, and Internet services is a privilege, not a right. Compliance with the Charter School's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may have their computer privileges limited and may be subject to discipline, including but not limited to suspension or expulsion per school policy.

Acceptable Use Agreement

The SAE believes that providing access to technology enhances the educational experience for students. However, student use of Charter School computers, networks, and Internet services is a privilege, not a right. To make that experience successful for everyone, students must abide by the following terms and conditions:

1. Security. Students shall not impair the security of Charter School technology resources. Students are expected to:
 - a. Safeguard all personal passwords. Students should not share passwords with others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised.
 - b. Access technology only with their account or with a shared account as directed by their teacher and not to allow others to use their account or to use the accounts of others, with or without the account owner's authorization.
2. Authorized Use. Students may use Charter School technology resources when directed by a teacher, when technology has been designated for open student use (e.g., computers in the library), and for other educational purposes.
3. Protection Measures. While the Charter School is able exercise reasonable control over content created and purchased by the Charter School, it has limited control over content accessed via the internet and no filtering system is 100% effective. Neither the Charter School nor its staff, employees, officers, directors or volunteers shall be responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes, misuse or negligence. The student and parent/guardian agree not to hold the Charter School or any Charter School staff, employees, officers, directors or volunteers responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes, misuse or negligence. They also agree to indemnify and hold harmless the Charter School, Charter School staff, employees, officers, directors and volunteers for any damages or costs incurred. Parents/guardians are required to supervise and monitor their child's use of The SAE equipment including but not limited to their child's access to the internet and any online services through such equipment any and all times during which any The SAE equipment is being used by their child outside school facilities or school hours to ensure compliance with this policy.
4. Inappropriate Use. Charter School technology, hardware, software and bandwidth are shared and limited resources and all users have an obligation to use those resources responsibly. Students are provided access to the Charter School technology primarily for educational purposes. Students shall not use Charter School technology or equipment for personal activities or for activities that violate Charter School policy or local law. These include but are not limited to:
 - a. Playing games or online gaming.
 - b. Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights.
 - c. Installing software on Charter School equipment without the permission of a teacher or other authorized Charter School staff person.
 - d. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.
 - e. Conducting any activity that is in violation of Charter School policy, the student code of conduct or local, state or federal law.
 - f. Engaging in any activity that is harmful to other student(s), including the use of technology to harass, intimidate, bully or otherwise disrupt the educational process.
 - g. Conducting for-profit business.
 - h. Using hacking tools on the network or intentionally introducing malicious code or viruses

- into the Charter School's network.
- i. Using any software or proxy service to obscure either the student's IP address or the sites that the student visits.
 - j. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.
 - k. Accessing or attempting to access material or systems on the network that the student is not authorized to access.
5. No Expectation of Privacy. Student acknowledges that computer equipment, Internet access networks, email accounts, and any other technology resources are owned by Charter School and provided to students for educational purposes. The Charter School may require staff to monitor and supervise all access to computer equipment, Internet access networks, and email accounts. To facilitate monitoring of activities, computer screens may be positioned so that they are visible to the staff member supervising the students. The Charter School reserves the right to access stored computer records and communications, files, and other data stored on Charter School equipment or sent over Charter School networks. Such communications, files, and data are not private and may be accessed during routine system maintenance; during inspection of Charter School equipment at the end of the school year/term or agree to use period; and review of individual files or monitoring of individual activity when there is a reasonable suspicion that the student is engaging in an inappropriate use.
 6. Disruptive Activity. Students should not intentionally interfere with the performance of the Charter School's network or intentionally damage any Charter School technology resources.
 7. Unauthorized Networks. Students may not create unauthorized wireless networks to access the Charter School's network. This includes establishing wireless access points, wireless routers and open networks on personal devices.
 8. Consequences of Inappropriate Use. Students who violate this Agreement will be subject to discipline, which may include loss of access to Charter School technology resources and/or other appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws.
 9. Technology Systems/Equipment Care. Students are not permitted to have food or drink near computers/other technology and must keep equipment and assigned areas free of vandalism.

After reading the Student Use of Technology Policy and the Acceptable Use Agreement, please complete this form to indicate that you agree with the terms and conditions provided. The signature of both the student and parent/guardian are mandatory before access may be granted to the technologies available. This document, which incorporates the Use Procedure, reflects the entire agreement and understanding of all parties. The SAE encourages parents/guardians to discuss this Policy with their children to ensure their children understand and comply with this Policy.

As a user of Charter School technologies, I have read Student Use of Technology Policy and hereby agree to comply with it and the Acceptable Use Agreement.

I understand that computer use is a privilege and not a right. I understand that students who violate this policy in any way will be subject to a referral and possible suspension or expulsion. I understand that if a student willfully damages The SAE's property, including but not limited to The SAE's technology, equipment and networks, or fails to return The SAE's property that has been loaned to the student, the student's parents/guardians are liable for all damages caused by the student's misconduct up to an amount not to exceed ten thousand dollars (\$10,000), adjusted annually for inflation. After notifying the student's parent or guardian in writing of the student's alleged misconduct and affording the student due process, The SAE may withhold the student's grades, transcripts, and diploma until the damages have been paid or

the property has been returned. If the student and the student's parent/guardian are unable to pay for the damages or to return the property, The SAE will provide a program of voluntary work for the minor in lieu of the payment of monetary damages. Upon completion of the voluntary work, the student's grades, transcripts and diploma will be released. A student over the age of majority shall be liable for the same. (Ed. Code § 48904).

Student Name (please print): _____ Grade: _____

Student Signature: _____ Date: _____

Parent/Guardian Name (Please Print): _____

Parent/Guardian Signature: _____ Date: _____

_____ **For School Employees Only** _____

I have read, understand and agree to abide by the Student Use of Technology Policy and the Acceptable Use Agreement. I understand that the Charter School's policies, procedures, rules, and regulations which apply to students also apply to me as an adult user of the Charter School's technology, in addition to any separate policies governing employee use of technology.

Employee Signature: _____

Employee Name (Please Print) _____