St. Andrew's Episcopal Academy
Acceptable Use Policy (AUP)

For the use of Computers, Mobile Devices, Internet Access, Apps for Education Internet Applications, and all other technologies

Maintaining the security and confidentiality of information and protecting Saint Andrew's Episcopal Academy (also referred to herein as the "Academy" or "SAEA") technology is a paramount concern of the Academy.

The Academy's concern in this regard is heightened by the various technology resources used by or provided to its employees to facilitate the creation and communication of business-related information in the most effective and efficient manner possible. In light of these concerns, this Policy has been developed, which establishes the parameters for technology resources usage and serves to enhance employee awareness of our obligation to hold certain information confidential, and to protect the integrity of the Academy's property and interests.

This Policy supplements all existing federal, state, local, laws, regulations, agreements, and contracts, and any other Academy policy, which currently apply to information confidentiality and technology resources. Users who do not comply with this Policy are subject to discipline, including, without limitation, revocation of technology usage and, up to and including, termination at the discretion of the Head of Schools.

Definitions

- User: Includes anyone, including employees, students, and guests, using SAEA technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products.
- Network: Wired and wireless technology – i.e. school networks, cellular networks, commercial, community or home-based wireless networks accessible to students.

- Equipment: Cellular phones, Smartphones, PDAs, MP3 players, iPod devices, desktop computers and portable computers such as laptops, iPads, tablets, as well as smart watches or portable storage devices, and/or all other technologies.

Technology provides students with unique and powerful ways to enhance learning. The Academy supports the use of technology for this purpose and is pleased to offer Users access to computer and cloud based networks.

One of the technology goals of SAEA is to ensure that each User's interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through SAEA-owned and/or student-owned devices inside or outside of our schools that degrades or defames other Users, or members of our community is unacceptable. SAEA also recognizes that Users have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity is considered to be included in this Acceptable Use Policy (AUP).

Disclaimer

This Acceptable Use Policy is a dynamic document and subject to revision. By accepting the terms as listed, you also agree to any changes made at any time.

Access

Access to SAEA's network is a privilege, not a right. The use of technology whether owned by SAEA or devices supplied by the Users entails personal responsibility. It is expected that Users will comply with SAEA rules, act in a responsible manner, and will honor the terms and conditions set by the classroom teacher, and SAEA. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental inappropriate use immediately to their teacher or school administration.

With the increased usage of free educational applications on the Internet, digital storage areas, containing less sensitive User information, may or may not be located on property of the Academy. Therefore, Users should not expect that files and communication are private. SAEA reserves the right to monitor Users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of SAEA property, network and/or Internet access or files, including email.

SAEA has a private and secure system for sensitive school records, which will be managed by SAEA, the office staff, and Administration. All devices are subject to search and seizure on demand per SAEA policies.

Safety

SAEA has taken prudent measures to protect students and employees using an educational Internet filter. SAEA will use this technology protection measure to block or filter, to the extent practicable, access of visual depictions that are obscene, inappropriate, and harmful to minors over the network. We require the registration of all devices brought on campus, including the students IP/MAC addresses, for this filter system.

In order for Users to gain access to their school email, SAEA must obtain parental permission for a minor under the age of 18 years. By signing this user agreement you are providing permission and holding SAEA and its representatives harmless from any and all liability involving such use by students, employees and guests. In addition, any user accessing SAEA technologies, network or services over the age of 18, is providing consent to abide by the Terms & Conditions of this AUP whether or not an AUP has been signed or is on file.

Terms and Conditions

These are examples of inappropriate activity on the SAEA network, but SAEA reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the SAEA network, Users, network or computer resources; 2) that expend SAEA resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by SAEA as inappropriate.

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting inappropriate pictures of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Frequent damage to equipment causing need to replace/repair more than a total of two (2) times.
4. Selling or purchasing illegal items or substances.
5. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
6. Causing harm to others or damage to their property.
7. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
8. Deleting, copying, modifying, or forging other Users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.
9. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.

10. Using any SAEA computer/mobile devices to pursue "hacking," internal or external to SAEA, or attempting to access information protected by privacy laws.
11. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."
12. Using web sites, email, networks, or other technology for political uses or personal gain.
13. Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
14. Advertising, promoting non-SAEA sites or commercial efforts and events
15. Users must adhere to all copyright laws.
16. Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

Repair Policy

The school is NOT responsible for loss, damage to, repair or replacement of, student-owned devices, regardless of where or when damage and/or loss occurs. In addition, students and staff are liable for mistreated, broken, or destroyed equipment and willfully developed or incapacitated technology or viruses, as well as other technical services caused by intentional misuse.

Cybersafety and Cyberbullying

All Users - Despite every effort for supervision and filtering, all Users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every User must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher, administrator, or system administrator.

Personal Safety – In using the network and Internet, Users should not reveal personal information such as home address or telephone number.

Confidentiality of User Information – Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.

Active Restriction Measures – SAEA will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are (1) obscene, (2) inappropriate, or (3) harmful to minors. Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. SAEA will also monitor the online activities of Users through direct observation and/or other technological means.

Interactive Web Tools

Technology provides an abundance of opportunities for Users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school(s). From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge are legitimate and safe. As the site is "public" and the teacher, school, and SAEA is not in control of it, all Users must use their discretion when accessing information, storing, and displaying work on the site. All terms and conditions provisions in this AUP also apply to User-owned devices utilizing the SAEA network.

Use of Interactive Web Tools

Online communication is critical to the students' learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. Student safety is the primary responsibility of teachers.

Therefore, teachers need to ensure the use of Documents, SAEA Moodle, classroom blogs, student e-mail, podcast projects, email chat features, or other Web interactive tools follow all established Internet safety guidelines including:

- The use of Docs, blogs, podcasts or other web tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web tools. This includes—but is not limited to—profane, racist, sexist, or discriminatory remarks.
- Users using Docs, blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- Users should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).
- Users should NEVER, under any circumstances, agree to physically meet someone they have met over the Internet, and should immediately report anyone trying to meet with them and/or any other suspicious behavior.
- Any personal blog created in class is directly linked to the class blog which is typically linked to the student profile and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use the blog login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and should follow these guidelines.
- Users should never link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.

- Users using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Users who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Student Use of SAEA and Personal Devices

- SAEA has provided some lower school students with devices to use while at school. The use of these devices follows the stipulations outlined in this AUP.
- School Administration and SAEA Technology staff may search and/or seize all student's and employee devices if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc. This includes the search of external hard drives, storage devices, cloud storage, and/or other cyber stored materials such as but not restricted to social media posts, blogs, etc.
- Users may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording as part of a school sponsored activity.
- These rules apply to student-owned devices as well.

Mobile/Cell Phone Policy

St. Andrew's Episcopal Academy recognizes and encourages the usefulness of cell phones and other devices as a means of supplementing educational instruction under staff supervision. These are the specific policies by user level:

User: Grades K-5

- Cell phones must be turned off and be put away from 8:00am-3:15pm. Under unique circumstances or learning situations, administrators may give permission to students or teachers.

User: Grades 6-8

- Cell phones must be turned off and be put away from 8:00am-3:15pm. Under unique circumstances or learning situations, administrators may give permission to students or teachers.

User: Grades 9-12

- Cell phones must be turned off during class, chapel, and other planned group activities and can only be turned on in the classroom with the teacher's consent. Students may use their cell phones outside of class time to place/receive phone calls or send/receive appropriate text messages.

If a student is found to have used a cellular phone without authorization or have used the device inappropriately he/she may receive the minimum of:

- *1st offense*: Phone will be confiscated by the staff member and may be given to administrator. Parent/guardian will be contacted and phone/device will be returned at the end of the school day or the next time parent is able to retrieve the device/phone in person.
- *2nd offense*: Phone will be confiscated by the staff member and given to administrator. Parent/guardian will be contacted and student will receive detention outside regularly scheduled school hours.
- *3rd offense*: Loss of campus phone privileges for the school term and/or semester.

However, administration reserves the right to set appropriate consequences based on severity of violation. Non-approved use of technology, including all cell phones will be dealt with according to the Acceptable Use Policy, including but not limited to expulsion from school or programs. The Academy is not responsible for any lost or damaged electronic devices and parents assume all liability for lost, stolen, damaged personal items. The parent also assumes all responsibility for any misuse of the phones and electronic devices by students, including visiting inappropriate sites, texting, cyber-bullying, or other misconduct as determined by the Head of School and/or designee administrator. Violation of the Acceptable Use Policy, may result in removal from school and/or programs.

Student Supervision and Security

- SAEA does provide content filtering controls for student access to the Internet using SAEA's network as well as reasonable adult supervision, but at times inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students. Students are to report the occurrence to their teacher or the nearest supervisor. Students will be held accountable for any deliberate attempt to circumvent SAEA technology security and supervision. Students using mobile and cellular devices while at school, during school, or other school-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use

Scope of the Policy for Other/ Non-Student Users

This Policy applies to all Saint Andrew's Episcopal Academy employees and other persons who are authorized to use the Academy's technology resources, including certain consultants, contractors, vendors, students, and interns ("users"). This Policy applies to the following forms of technology resources and the information created by their use, including but not limited to (1) computers (including desktop, laptops, portable, servers, mainframes, local area networks, wide area networks, printers, software and removable storage media (e.g., CD-ROMs, flash drives and tape)); (2) electronic mail ("e-mail"), including attachments; (3) the Internet, (4) the phone systems, and (5) anything connected to or apart of the Academy's server. The term "the Academy's Technology Resources" is meant to include any of the aforementioned, specifically, and any other computer-related or technology-related device that is or may be owned, rented, or leased by the Academy.

- Guests may access the "Guest Wifi" using a password available through the front office.
- Guests to campus, volunteers, and chaperones are requested to silence cell phones and put away while on campus. If you are here to visit classrooms or programs, to supervise, monitor or assist with the students in any way, then your attention should be on the students. In case of an emergency, please step away from the students and make sure another adult has assumed authority for the student care.

- Employees and Contracted Services Personnel should refer to employee policies, contracts and other such documents for more specific guidelines concerning their acceptable use of technology, phones, devices on campus.

The Policy

1. The Academy's Technology Resources May Be Used Only For Legitimate, Business-Related Reasons.

   The Academy's technology resources may be used only for legitimate business-related reasons. The Academy's technology resources may not be used to conduct personal business of any kind, without expressed permission from a supervisor or administrator at the Academy. All information that is entered, created, received, stored or transmitted via the Academy's technology resources, including all e-mail messages, are and will remain the Academy's property. Such information may neither be used for any purpose unrelated to the Academy's business nor sold, transmitted, conveyed or communicated in any way to anyone outside of the Academy other than for business-related reasons.

2. No Expectation of Privacy

   Users should have no expectation of privacy in connection with the entry, creation, transmission, receipt, or storage of information via the Academy's technology resources. Users waive any right to privacy in information entered, created, received, stored or transmitted via the Academy's technology resources, and consent to access and disclosure of such information by authorized personnel.
   As with all other property, the Academy's technology resources and all information entered, created, transmitted, received or stored via our technology resources is subject to inspection, search and disclosure without advance notice by persons designated or acting at the direction of the Academy or as may be required by law or as necessary to ensure the efficient and proper administration and operation of our technology resources. For example, authorized persons may inspect, search and disclose such information to investigate theft, disclosure of confidential business or proprietary information, personal abuse of the system, or to simply monitor work flow or productivity. This monitoring and/or search includes, without limitations, the individual hard drives of any computer owned, leased, rented, or maintained by the Academy, any information stored on any hard drives owned, leased, rented, or maintained by the Academy, which may include emails to or from any Academy issued email account, or any personal account that may be accessed from a the Academy computer, any documents drafted on the Academy's computer, any internet sites accessed, and/or any phone calls made or received from any

phone systems owned, leased, rented, or maintained by the Academy, and any messages left on any phone owned, leased, rented, or maintained by the Academy.

Because the Academy is sensitive to employee concerns, it will make every effort to ensure that all such inspections are conducted professionally and ethically. Users, however, must recognize that authorized persons have the ability to track and monitor all information sent internally and externally to the Academy via technology resources at any time for any reason.

Users should have no expectation of privacy in any of the work that is performed on any Academy computer, with any emails transmitted or received (or accessed) on a Academy computer, any internet site accessed on a Academy computer, or with respect to any phone call received or made to/from any Academy phone system, or any messages left on any Academy phone system. All passwords and security used in connection with the Academy's technology resources are the Academy's property and must be available to the Academy's, upon request, for any reason. Users should understand that their use of passwords does not preclude authorized persons to access the Academy's technology resources.

3. The Creation or Transmission of Any Information That May Be Construed To Violate the Academy's Harassment-Free Workplace Policy or Equal Employment

   Opportunity Policy Is Strictly Prohibited Users are strictly prohibited from using the Academy's technology resources in any way that may be offensive to others. This prohibition includes, for example, the transmission of sexually explicit or obscene messages or cartoons, ethnic or racial slurs, or anything that may be constructed unlawful harassment or disparagement based on race, color, religion, sex, national origin, age, disability, ancestry, sexual orientation, marital status, parental status, source of income, military discharge, or any other status protected by law. Relatedly, users may not use technology resources to transmit critical or derogatory statements regarding individual employees, clients, consultants, contractors, vendors, students, volunteers or residents. Users violating these prohibitions may be subject to disciplinary action, up to and including termination at the discretion of the Head of Schools.

4. Use of the Academy's Technology Resources Is Subject To the Academy's No Solicitation/No-Distribution Policy

   The Academy's policy strictly forbids employees from soliciting, during their working time or the working time of the employee being solicited, any other employee to support any individual or organization. It also forbids employees from distributing any literature on behalf of any individual or organization on Academy property. This includes the distribution of chain letters of all kinds, this includes political campaigns, and other such communications and distributions.

5. Intellectual Property (Copyright and Patent) Laws and Computer Standards

   Users may not violate any copyright, patent or other intellectual property law, including restricted software laws. Accordingly, unless permission has been expressly and officially provided, users may not post or download any information protected by copyright or

patent law. If copyright, patent or other ownership status is unknown, users may not post, upload, download or otherwise use any information, content, software or other property and should consult the network administrator with any inquiries.

6. Viruses

All Academy technology resources must be protected from accidental destruction or deliberate attempts at sabotage by computer viruses. Users thus may not introduce virus-infected files or media into the Academy's technology resources. Users must make all reasonable efforts to ensure that all files accessed or collected are virus-free and should minimize downloading work-related information unfamiliar from the Internet and via e-mail. Users should use discretion when receiving e-mail from unknown sources, especially where the e-mail contains attachments. Prior to placing any file on the Academy's network, users must scan for viruses using up-to-date, approved virus scanning software.

7. Confidential Information

Users must take every measure to ensure that confidential Academy's information, and information otherwise protected is entered, created, received, stored or transmitted via technology resources remains confidential and private. Likewise, users must continue to respect the confidentiality of any report containing confidential information while handling, storing, and disposing of these reports in an appropriate manner. Users are prohibited from searching for using, sending, posting or otherwise disclosing confidential information or information protected by the attorney-client privilege to any individual for any non-work or business related reason, without partner permission from Head of Schools and in accordance with requirements of Privacy Laws.

8. Encryption

To ensure continuous access to technology resources users shall not use personal hardware or software to encrypt information entered, created, received, stored or transmitted via technology resources.

9. Internet Use

Like all other technology resources, the Academy provides Internet access only for legitimate business-related, education, research, outreach, and administrative purposes. The Internet shall not be used for any personal use during hours when students/classes are in session.

10. Social Media

Social Media includes any website or medium (including video) that allows for the electronic and digital communications in cyberspace, which includes, but is not limited to, email, internet, text messaging, Facebook, Twitter, LinkedIn, YouTube, and blogs. A policy has been developed to protect you and the Academy's exposure and liability, while also providing you an opportunity to share educational forums and ideas with others. The use or accessing of social media at work is not permitted without expressed written authorization from a supervisor or administrator for non-academic purposes.

When using social media within a written authorization through the Academy, or using social media outside of working hours on your own time, any use must be consistent with our mission, purpose, and values. All employees must use social media within the guidelines set forth in the employee handbook and/or rules of conduct. Violations of the the policy, no matter how small, can and will be subject to discipline as outlined fully in the employee handbook.

You are personally responsible for what you post. Remember that what you post can often be viewed by both personal and professional contacts. Post responsibly. If you publish content related to the Academy on any non-Academy operated or sponsored site, you must state that "the views on this post are my own and not necessarily those of Saint Andrew's Episcopal Academy.

Photographs of students may not be released or published on personal social media by employees. Only the school sites may release photos of school activities and students.

Additionally, with all posts on any social media site you must abide by the following:
• Do not publish any confidential or proprietary information on a social site;
• Do not discuss the Academy, the Academy employees, vendors, clients, or other partners of the Academy, without written authorization;
• Do not use insults, obscenity, racial slurs, ethnic slurs, or any other negative comments that can be construed in any way as discriminatory or harassing;
• Do not post photographs taken at any Academy-sponsored events, including picture of students and/or employees; and
• Respect all copyright, fair use, and financial disclosure laws;

11. Other Communications

Communications between school personnel and students outside of school shall be limited to traditional, organization-authorized methods such as SAEA issued email accounts, and should only be conducted for SAEA related purposes. Accordingly, the following communication and contact between SAEA personnel and students is prohibited:

• Calls to a student's personal phone,
• Texting,
• Communication through messaging services such as Instant Messenger,
• Communication through personal social networking accounts, including "friending," and
• Communication through personal email accounts.

Should communication outside of traditional, or authorized methods be necessary, the administration should be notified of the communication and its purpose, and the communication should be documented by the personnel member.

12. Violations

Violations of any of the above policies by personnel shall be subject to discipline, up to and including, termination or expulsion.