Required Use Policy

Saint James School
STUDENT REQUIRED USE AND INTERNET SAFETY POLICY (RUP)
(in accordance with Children's Internet Protection Act [CIPA]and Alabama Public Law Article 5 Section 13A)

PURPOSE:
Saint James School provides all students access to the Internet, network resources and MacBooks, iPads, and iPod Touches at designated grade levels, as a means to promote achievement and provide diverse opportunities during the educational experience. This policy provides guidelines and information about the limitations that the school imposes on use of these resources. In addition to this policy, the use of any school computer, including MacBooks, iPads, and iPod Touches, also requires students to abide by the Saint James School Technology Use Guidelines as stated in the Student Handbook. We expect our students to exercise good judgment and to utilize technology with integrity. Rules may be added as necessary and will become a part of this policy.

TERMS OF THE REQUIRED USE AND INTERNET SAFETY POLICY
Specifically, the student:

- Will adhere to these guidelines each time the Internet is used at home and school.
- Will make available for inspection by an administrator or teacher upon request any messages or files sent or received at any Internet location. Files stored and information accessed, downloaded or transferred on school-owned technology are not private.
- Will use appropriate language in all communications avoiding profanity, obscenity and offensive or inflammatory speech. Cyber Bullying such as personal attacks and/or threats on/against anyone made while using school owned technology to access the Internet or local school networks are to be reported to responsible school personnel. Rules of netiquette should be followed conducting oneself in a responsible, ethical and polite manner. This includes email, texting messaging, and chatting.
- Will follow copyright laws and should only download/import music or other files to a school owned technology device that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.
- Will never reveal identifying information, files or communications to others through email or post to the Internet.
- Will not attempt access to networks and other technologies beyond the point of authorized access. This includes attempts to use another person's account and/or password as well as torrents or proxies.
- Will not share passwords or attempt to discover passwords. Sharing a password could make you liable if problems arise with its use and subject to disciplinary action.

- Will not download and/or install any programs, files, or games from the Internet or other sources onto any school owned technology. This includes the intentional introduction of computer viruses and other malicious software, as well as the installation of any iOS or OS upgrades without prior approval.

- Will not tamper with device hardware or software, unauthorized entry into devices, and vandalism or destruction of the device or device files. Damage to devices may result in felony criminal charges. It is the responsibility of the student/family to pay for damage to the school owned device.

- Will not attempt to override, bypass or otherwise change the Internet filtering software or other network configurations. This includes the use of torrents and 'private browsing'.

- Will use technology for school-related purposes only during the instructional day while refraining from use related to commercial, political or other private purposes. This includes shopping and play ing games.

- Will not make use of materials or attempt to locate materials that are unacceptable in a school setting. This includes, but is not limited to pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school media center. Specifically, all school owned technologies should be free at all times of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials (files).

- Will not connect any personal technologies, wireless access points and routers, printers, etc to the school owned and maintained local area network. Home Internet use and cost is the responsibility of the student/family both in cost and configuration. Dial-up is not an option as recent configurations do not include modems. The use of printers from home is permissible but is the responsibility of the student to configure.

- Will not sync personal smart devices (iPhones, Android phones, Kindles) to school owned computer.

- Will keep device secure and damage free. Each device is issued with a protective book bag or case.

- Will backup data and other important files regularly. Saint James School will at times maintenance the devices by imaging. All files not backed up to a "cloud" storage space or other storage media will be deleted during these processes. Students are ultimately responsible for backing up all personal files on their own storage space.

- Will have a school issued Apple ID to store data to iCloud (for middle school iPads). Student's are not to install apps. The technology department may issue exceptions.

- Will have a school issued Apple ID to install school approved apps to their school issued computer. (High School).

- Will use the provided device backpacks & cases for computers and cases for iPads and is required at all times.

Keep the device secure and damage free:

- Do not loan your device or charger and cords.
- Do not leave the device in a vehicle.
- Do not leave your device unattended.
- Do not eat or drink while using the device or have food or drinks in close proximity to the device.
- Do not allow pets near your device and power cords.
- Do not place the device in floor or in sitting area such as couches or chairs.
- Do not leave the device near table or desk edges.
- Do not stack objects including books on top of your device.
- Do not leave the device outside or use near water such as a pool.
- Do not check the device as luggage at the airport.
- Devices must be carried and transported appropriately on campus. They should be carried in their approved cases/backpacks at all times.
- Devices must be in a student's possession or secured in a locked classroom or locker at all times.
- Do not borrow a device from another student.
- Device must not be taken into restrooms.
- Devices must be carried and transported appropriately on campus. They should be carried in their approved cases at all times. Failure to close the lid of a device before transporting will damage the hinge and could damage the hard drive and result in permanent loss of data.

Note: Students are entirely responsible for backing up their own data. Lost or damaged data is not the responsibility of the school. All school–issued Devices must be in the school–issued case.

- Devices may not be used in the PAB during lunch.
- Devices should be handled with respect and care. Inappropriate treatment of school devices is not acceptable. Any damage costs are the responsibility of the student/family.
- Devices are not to be written on, to have stickers applied to them, or to be defaced in any way.
- Don't remove, move or write on the identification sticker on your device.
- In the unfortunate event that your device is stolen, contact the police and the school immediately. Ultimately, it is the responsibility of the student/family to look out for and protect their device as well as the cost for a replacement device.

*Any costs incurred because of damage not covered by Apple Care Warranty is the responsibility of the student/family.

Internet Use

- The Internet is a rich and valuable source of information for education. 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.
- Information obtained through the Internet must be properly cited and in compliance with copyright laws. Due to the quickly changing nature of the Internet, a hard copy of referenced material is recommended.
- Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

- Plagiarism includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.
- If a student accidentally accesses a website that contains obscene, pornographic or otherwise offensive material, he/she is to notify a teacher, the Technology Director, or the Principal as quickly as possible so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

EMail

- Every student will have a school email address with the stjweb.org domain. Emails can only be sent and received to this domain unless authorized by faculty or administration. School email should not be used for personal reasons.
- Students WILL NOT set up personal emails on school owned devices. Saint James devices are for school use only.
- The use of email during class is prohibited unless authorized by faculty or administration.
- Students should always use appropriate language in their email messages.
- Email etiquette should be observed. In general, only messages that one would communicate to the recipient in person should be written.
- Email services provided by the school are to be used only for the exchange of appropriate information.
- No inappropriate email is allowed including derogatory, obscene, or harassing messages. Email messages of an abusive or harassing nature will be regarded as a major violation and will be subject to a disciplinary response.
- Chain letters of any kind, phishing, or spam are prohibited. Chain letters are defined as any email message asking you to pass information or messages on to other individuals or groups via email. Phishing is a fraudulent attempt to steal your personal information, such as passwords, account information, or user names. Spam is use of electronic messaging systems to send an unsolicited message (**spam**), especially advertising.
- Students are prohibited from accessing anyone else's email account.
- Only approved mail programs may be used for student mail.
- School email addresses are not to be given to ANY websites, companies, or other third parties without the explicit permission of a teacher or administrator.
- Only school–related attachments may be sent on the school email system.

Chatting, Messaging, and Blogging

- Instant messaging is prohibited on campus except as part of an assigned, in-class activity that is supervised by faculty or administration. This includes any parent communication using internet email chat applications.
- Blogging is to be utilized on campus only for academic purposes.
- Participation in chat rooms during school hours is prohibited during the school day, except as part of an assigned, in-class activity.

Audio and Video

- Audio on devices should be turned off unless required for the activity being conducted.
- Listening to music either aloud or with earphones is not permitted on campus unless required for the activity being conducted. Faculty and staff may relax this policy at their discretion.
  **The use of cell phones is prohibited per the Saint James Student Handbook. (p.17)
- When sound is needed, headphones provided by the student must be used.
- The use of devices to watch movies or stream movies and/or music, unless assigned by a teacher, is not permitted during the school day.

- Any audio or video recording may be done only with the prior permission of all parties being recorded.
- Sharing of music (including iTunes music sharing) over the school network is strictly prohibited and is subject to appropriate consequences.

Games
- The view and/or playing of electronic games is not permitted during school hours except as part of an assigned, in-class activity.
- Any internet games, virtual games, or games accessed through an external or USB drive is prohibited.
- The school reserves the right to remove any game from a school computer that is considered inappropriate or impedes the educational purpose of the device program.
- No games that are "played" over the school network are allowed.
- Games that include violence, adult content, inappropriate language, and weapons are not to be installed or "played" on school Devices.
- Screensavers that include gaming components are not allowed.

Network Access
- Students must not make any attempt to access servers or network information that is not open to the public.
- The utilization of proxy avoidance IP numbers and programs is strictly prohibited. This includes Torrents, BitTorrents and the like.
- Connected school devices to a personal hotspot while on campus is strictly prohibited and will result in immediate **detention**.
- Students may not use the school network for personal or private business reasons including but not limited to online ordering and purchases.
- 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.
- Saint James School is not responsible for damaged or lost data transferred through our network or stored on Devices, computers, or our file servers.

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 considered file sharing.
- File sharing of any kind is prohibited both on campus and off campus. The only exception to this is when it is a specific assignment given by a faculty member.
- Remotely accessing a personal computer is strictly prohibited.
- No file sharing software of any kind is to be installed on school computers including Devices. Examples of this type of software are Limewire, Frostwire, Kazaa, iMesh, etc. Although these types of programs are software downloads, they automatically create file sharing connections.
- There is a $25 re-imaging charge to get rid of any unapproved software or files.

Deleting Files
- Do not delete any folders, files, or apps that you did not create or that you do not recognize. Deletion of certain files or apps may result in a device failure and will interfere with your ability to complete class work and may affect your grades.
- There is a $25 re-imaging charge to correct system files.

Downloading and Loading of Software

- Downloading and Loading of Software is Blocked. Students are not permitted to install any software.
- There is a $25 re-imaging charge to get rid of any unapproved software or files.

Screensavers and Wallpapers

- Inappropriate or copyrighted media may not be used as a screensaver or wallpaper.
- Presence of weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures will result in disciplinary actions.
- Do not place a passcode or Touch ID on school issued iPad.
- There is a $25 re-imaging charge to remove any of the above.

Privacy, Use, and Safety

- Students may not give any personal information regarding themselves or others through email 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 email 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 device access. This is important in order to protect the privacy of each student. Do NOT share personal passwords or usernames.
- Saint James School respects the privacy of every student, faculty member, and administrator with respect to stored files and email accounts. However, if inappropriate use, including honor code violations or harassment, are suspected, the school administration has the right to view these files in order to investigate suspected inappropriate behavior.
- 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 prohibited from accessing faculty, administration, and staff computers as well as school file servers for any reason without explicit permission from the user or administrator of that computer.
- Students are prohibited from utilizing the Terminal interface. In addition to this, students are prohibited from using any method to obtain control of another person's computer through the use of their own computer.
- Students are prohibited from utilizing peer-to-peer networking or any method of file sharing between computers, such as AirDrop, unless authorized by the technology staff.
- No identifiable photographs of students, faculty, or administration will be allowed to be published on the Internet or used in print without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.
- Cyberbullying is the use of electronic information and communication devices to willfully harm either a person or persons through any electronic medium, such as text, audio, photos, or videos. Examples of this behavior include but are not limited to:
  - Sending/posting false, cruel, hurtful or vicious messages/comments;
  - Creating or contributing to websites that have stories, cartoons, pictures, and jokes ridiculing others;
  - Breaking into an email account and sending vicious or embarrassing materials to others;
  - Engaging someone in electronic communication, tricking that person into revealing sensitive personal information and forwarding that information to others;

- Posting of a student picture without their permission;
- Any electronic communication that creates a hostile, disruptive environment on the school campus is a violation of the student's and staff member's right to be safe and secure. Actions deliberately threatening, harassing, intimidating an individual or group of individuals; placing an individual in reasonable fear of harm; damaging an individual's property; or disrupting the orderly operation of the school will not be tolerated.

Devices that are provided by the school continue to be the property of the school. Therefore the school has the right to view all content at any time. Any electronic device used on the school network, even if privately owned, is subject to all policies and consequences of the Required 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 RUP that deserves that consequence.

Copyright

- Unauthorized duplication, installation, alteration, or destruction of data programs, hardware, or software is prohibited.
- Data, apps, programs, hardware, software, and other materials including those protected by copyright may not be transmitted or duplicated.

Consequences

- The school reserves the right to enforce appropriate consequences for the violation of any section of the Required Use Policy. Such consequences could include the loss of privileges on a device, the loss of the use of the computer for an amount of time determined by the administration and members of the Technology Department, possible disciplinary action, and possible legal action.
- Faculty members have the right to issue infractions if any students appears to have violated any part of the RUP. Faculty members may also take up the device and turn it into the school's principal or the Director of Technology.
- Computers with illegal or inappropriate software or materials on them will be reformatted or "re-imaged," and the student will be charged a $25 RUP violation fee PER incident for this service. This amount may be increased for repeat violations.
- In the case of repeated device abuse and/or damages, the school has the right to revoke the use of the school's device and the student will be restricted to using only on-campus computers. Repeated RUP offenses or device abuses may lead to the loss of a student's privilege of using any device on campus.
- Students are to report any known violations of this Required Use Policy to appropriate administrative staff members. Random checks of student Devices will be conducted throughout the year to ensure that these policies are being followed.
- Saint James School takes no responsibility for activities conducted on school computers and Devices or materials stored on computers, Devices, or the school's network.

By signing this you agree to abide by the conditions listed above and assume responsibility for the care and proper use of Saint James School technology, including personally backing up personal data and any physical damage. Saint James School is not responsible for any loss resulting from delays, non-deliveries, missed deliveries, lost data, or service interruptions caused by user errors, omissions or reasons beyond the school's control. Information obtained via the Internet and other sources using Saint James School's technologies is not guaranteed as to its accuracy or quality. I understand that should I fail to honor all the terms of this Policy, future Internet and other electronic media accessibility may be denied. Furthermore, I may be subject to disciplinary action outlined in the Saint James School Student Code of Conduct and, if applicable, my device or iPad may be recalled. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet under the conditions set forth above as well as agree to pay any charges not covered by Apple Care Warranty program.

As the parent/guardian, my signature indicates I have read and understand this Required Use Policy, and give my permission for my child to have access to the described electronic resources.

Parent/Guardian (please print): _____

Parent/Guardian Signature: _____Date: _____

As the student, my signature indicates I have read or had explained to me and understand this Required Use Policy, and accept responsibility for abiding by the terms and conditions outlined and using these resources for educational purposes.

Student (please print): _____

Student Signature: _____Date:_____
Terms and Conditions: This RUP is valid through June 30, 2018