ST. JAMES STUDENT ACCEPTABLE USE POLICY

St. James Episcopal Day School (SJEDS) recognizes that as telecommunications and other technologies change, there will be a shift in the ways in which information may be accessed, communicated, and transferred by members of our society. Methods of instruction and student learning will also change. Guidelines are provided below to make all SJEDS technology users aware of the responsibilities that they accept when they use SJEDS resources. In general, what is required is efficient, ethical, and legal utilization of technology resources on the SJEDS campus - use that is respectful of the rights of all users in the school community.

Appropriate Use of Technology Resources

SJEDS provides technology to support the pursuit of educational excellence by its students. Within the school environment, technology is to be used to create, provide diagnostic information, research/information, and to foster positive engagement as a digital citizen. Uses that might be acceptable in another environment may not be acceptable in this system because of its limited educational purpose or other inappropriateness.

Procedure for Reporting Inadvertent Inappropriate Use

If a user inadvertently uses a technology resource inappropriately, the user is responsible for immediately notifying a teacher or an administrator of the mistake. Failure to report unintentional misuse may result in the incident's being considered an intentional violation.

Unacceptable Use of Technology

SJEDS seeks to protect the civil, personal, and property rights of those individuals using school technology resources and regards the following technology use as unacceptable:

Accessing Information Which Does Not Support Educational Purposes

- Sexually explicit sites
- Hate or discrimination sites
- Sites that promote violence or illegal activities
- Sites that promote or support academic dishonesty
- Any Social Media not approved by the Technology Department to be compliant with state & federal regulations
- Use of proxies or anonymizers to access sites to circumvent any network security measures set in place
- Use of any personally owned digital technology brought to campus without prior approval from administration

Publishing (Sending, Forwarding, Posting) Inappropriate Information

- Communications of any kind containing language that is obscene, profane, sexually explicit, lewd, vulgar, rude, disrespectful, threatening, or inflammatory
- Communications of any kind containing harassment, personal attacks (including prejudicial or discriminatory), or hate mail (spreading false or defamatory material about a person or organization). This also includes any form of cyber bullying
- Sending (including forwarding) chain letters or spam (annoying or unnecessary messages to large numbers of people)
- Posting to Social Media or other web pages in a way that connects students to SJEDS without prior approval from administration (including pictures or video)

Abusing Technology Resources

- Using the network in ways that disrupts network use by others
- Using the network to engage in illegal activity
- Changing, rearranging, adding, or deleting software settings on school resources
- Downloading, installing, or storing unauthorized software or other files on school systems
- Downloading or storing files or other information on the hard drive of a school computer rather than the approved network location
- Wasting finite resources; i.e., print cartridges and paper by printing unnecessarily, bandwidth or data storage by downloading or storing unnecessary content
- Using school technology resources to conduct a business or for other unauthorized commercial gain
- Using school provided services to sign up for any services not approved by SJEDS
- Loss of charger charger cable, charger plug, or any other issued technology
- Playing video games without permission from teacher or administrator (this includes all games, including online educational games that are not part of a classroom assignment)
- Using any personal technology for non-academic purposes without permission during school hours
- Using any school provided technology for non-academic purposes without permission at any time without permission

Safety and Security Issues

- Failing to keep personal passwords confidential
- Using the password of another person
- Misrepresenting yourself or someone else online
- Disclosing photographs, video, audio or other personal information, such as names, addresses, or phone numbers, online for the school, for oneself or for others without school permission
- Entering credit card numbers and purchasing materials or services online
- Hacking or otherwise accessing accounts of others even if the location is left unlocked
- Spoofing or otherwise falsifying the source of network traffic
- Creating or propagating computer viruses or overloading the school's network resources

Copyright/Piracy Issues

- Downloading or exchanging pirated or illegally obtained software
- Violating software licensing agreements by loading software illegally
- Copying, modifying, distributing, displaying, or transmitting the work of another without contacting the owner for permission (material on most websites is protected by copyright)
- Cracking/spreading or otherwise copying or distributing commercial software

Policy on Cyberbullying

As also found in the student handbook, cyberbullying (tormenting, threatening, harassing, humiliating, embarrassing or otherwise targeting others using the internet and/or digital technologies) will not be tolerated. Disciplinary and appropriate legal action will be taken for students who violate this policy through the use of technology to protect others in our community.

Consequences for Inappropriate Use

Access to technology is provided as an important component of the educational environment. Users who fail to adhere to the terms of the Acceptable Use Policy face disciplinary action outlined in the SJEDS behavior policy.

Disclaimers

SJEDS makes no warranties of any kind, whether expressed or implied, for the Internet access service it provides. SJEDS specifically denies any responsibility for the quality of information obtained through the Internet. SJEDS denies responsibility for loss of data resulting in delays, non-deliveries, miss-deliveries, or interruptions sustained by users as a result of system failure. SJEDS denies responsibility for financial obligations arising from unauthorized use of the system for the purchase of products or services. SJEDS accepts no responsibility for damages incurred by a user's inappropriate use of the system. SJEDS may act as an agent for parents under COPPA (Child Online Privacy Protection Act) for cloud services (SaaS), including school-related online programs, mobile device application sign-up, and all other aspects of the school's policy on student Internet usage for academic purposes which require direct parent consent. ***This consent is granted with the signing of the school enrollment contract.***

Limited Expectation of Privacy

Users of SJEDS technology resources have the right to privacy from their peers; however, SJEDS administration reserves the right to gain access to these files to investigate unusual activity on the system or any user believed to be in violation of acceptable use guidelines.

Although the Internet is a very worthwhile educational tool, it poses the risk of its users being exposed to inappropriate materials. SJEDS focuses on students' learning to make appropriate choices based on school guidelines and personal values. Campus Internet use is monitored so that users making inappropriate choices can be redirected toward productive use in accordance with school guidelines.

Parents/guardians have the right at any time to investigate or review the contents of their child's files while on campus and by request in accordance to FERPA (Family Educational Rights & Privacy Act) requirements.

ST. JAMES
EPISCOPAL DAY SCHOOL

Technology Policies Signature Page

This page requires a signature from a parent/guardian for all students at St. James Episcopal Day School. In addition, it requires the signature of a student if they are going into the third, fourth, or fifth grade for the 1:1 iPad program.

This section to be completed by students in third, fourth, and fifth grade only

Select a grade level: 3rd_____ 4th_____ 5th_____

The student agrees to and will follow the policies outlined in the iPad Handbook, the Acceptable Use Policy, and any other additional policies covered in other areas of the St. James Student Handbook or Community Guidelines pertaining to technology for the 2019-2020 school year at St. James Episcopal Day School.

Student Signature _____

Date _____

Where applicable, parents/guardians agree and will abide to the policies stated above for the 2019-2020 school year.

Parent/Guardian Signature _____

Date _____