Electronic Communications and Responsible Use Policy 2016 -2017

St. George's is committed to the use of technology in the academic program as a tool to expand learning opportunities and conduct academic research. The use of technology facilitates global collaboration, creativity, communication, and critical thinking, all of which are vital skills for our learners. Students utilize computers on a wireless network. Laptops, campus computers, and iPads are for educational use consistent with the educational goals of St. George's Independent School. Along with this opportunity comes responsibility. The Responsible Use Policy is designed to give students and their families clear and concise guidelines regarding the appropriate use of laptops as well as other computers or mobile devices. The examples below are just examples and are not an all-inclusive list of requirements or possibilities. The underlying premise of this policy is that all members of the St. George's community must uphold the values of honesty and integrity as part of the school's honor code. The proper use of technology reflects the strength of one's character, as does one's behavior. We expect our students to use good judgment and to utilize technology with integrity.

Whether physically on campus or off campus, whether during the school day or at night, on vacation or at any other time while enrolled at the school, whether linked to the school's network from in school or from a remote location or not at all, or using a personal or computer or communication device on or off campus, students are expected to comply with this Responsible Use Policy and any other applicable policies and procedures as long as they are enrolled at the school, as set forth in this Handbook and as further described below.

Terms and Conditions

Email

- Email during class is prohibited unless authorized by faculty or administration.
- Students should always use appropriate language in their email.
- 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 violation of a major school rule and will be subject to a disciplinary response.
- Chain letters of any kind and 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.
- Students are prohibited from accessing anyone else's email account without first receiving explicit permission from the account holder.
- Email etiquette should be observed. In general, only messages that one would say to the recipient in person should be written.
- Only the school email accounts are to be used for school communication.
- 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.
- The school reserves the right to search and read email as deemed necessary.
- Only school–related attachments may be sent on the school email system.

Online Services and Social Media

- Instant messaging is prohibited on campus except as part of an assigned, in-class activity that is supervised by faculty or administration.
- Blogging, tweeting (Twitter), and the use of other social media is to be utilized on campus for academic purposes only.
- Participation in chat rooms is prohibited during the school day, except as part of an assigned, in-class activity.
- Students access online resources such as Glogster, Discovery Education, Turnitin.com, etc. as part of their academic work. These resources sometimes require the utilization of student information such as a student's name and school email address. These websites typically provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. St. George's Independent School has the right to consent to the collection of personal information on behalf of all of its students, and will do so, thereby eliminating the need for individual parental consent given directly to the web site operator.
- Students may not be "friends" with, or otherwise be directly or indirectly connected to, any school employee on any social networking site that is not primarily used for educational purposes. If a student is contacted by a school employee via non-school channels for non-educational purposes, the student should immediately notify the student's Division Director.

Audio, Video, and Photos

- Audio on computers and mobile devices should be turned off unless required for the activity being conducted.
- Listening to music either aloud or with earphones is not permitted during class or study hall unless specifically approved by a faculty member. Listening to music during free periods or other times while on campus is permissible unless it is disruptive to the activities taking place. Faculty and staff can restrict this at their discretion.
- The use of laptops, desktops, or mobile devices to watch videos is not permitted during the school day except as part of an assigned, in–class activity.
- Any audio, video recording, or capturing of photos may be conducted only with prior permission of all parties being recorded or photographed.
- Sharing of music (including iTunes music sharing) over the school network is strictly prohibited.

Games

- Electronic games are not permitted during school hours except as part of an assigned, in-class activity.

- The school reserves the right to remove any game from a school computer that is considered inappropriate or that impedes the educational purpose of the academic program.
- Games that include violence, adult content, inappropriate language, and weapons are not to be installed or played on student or school computers, laptops, or other electronic devices.

Laptops, Computers, and Other Electronic Devices

- Students must maintain the original configuration of all school-owned computers and iPads; this includes not altering the appearance of the desktop, dock, windows, or control panels/system preferences.
- All laptops utilized at the Collierville campus, whether personally owned or obtained through the school laptop program, are expected to be in good working order at all times. Loaner laptops are only available to students who purchase their laptop through the school laptop program.
- Student laptops, iPads, and other electronic devices must not be left unattended at any time. If any of these items are found to be unattended, they will be turned in to the Laptop Center on the Collierville campus or the Technology Office at the Lower School.
- Laptops and other electronic devices must be in a student's possession or secured in a locked cart, locked classroom, or locker at all times.
- Laptops and other electronic devices must be transported appropriately on campus. They should be carried in their cases if at all possible. Otherwise, laptops should be closed and carefully carried. Failure to close the lid of a laptop before transporting it 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.
- No food or beverages should be in the vicinity of computers, laptops, iPads, or other electronic devices, and they may not be used in the dining hall during lunch.
- Laptops, iPads, and other mobile technology devices should be handled with respect and care. Inappropriate treatment of these devices is not acceptable.
- Students are not allowed to create any bios passwords on their laptops (bios passwords are set through the computer's hardware and are not the same as regular passwords).
- In the case of theft of a school–issued laptop, a police report must be filed, and a copy of the police report (which must include the serial number of the laptop) must be submitted to the Laptop Center staff in order to process the insurance claim.
- Students may not intentionally vandalize, steal, or cause harm to any school-owned equipment, or remove any school-owned equipment from campus.

Cell Phones and Mobile Electronic Devices

- Students are not permitted to use cell phones and other electronic devices on campus during the academic day (or in after-school care on the lower school campuses) unless prior approval for utilizing the device during a specific time period or class is given by a faculty or staff member. All such devices must be turned off or placed in silent mode unless such permission has been granted, though upper school students may use their phone to check school e-mail. Note: St. George's Independent School is not responsible or liable for loss, theft, or damage related to students' personal mobile devices.
- Wearable technology devices, such as smart watches, are covered by the same policies as cell phones and other mobile devices, including being placed in silent mode at all times. Additionally, they are required to be removed during tests, exams, or when requested by faculty or administrators.
- Google Glass is prohibited.

Network Access

- Students must not make any attempt to access servers or network information that is not open to the public.
- Students may not access or make any attempt to access network resources not intended for them.
- The utilization of proxy avoidance IP numbers and programs (including browser extensions) is strictly prohibited.
- Students may not create or use a mobile hotspot on the school campus.
- Students may not use the school network for personal or private business reasons.
- 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, and attempting to gain access to restricted or unauthorized network services.
- St. George's Independent School is not responsible for damaged or lost data transferred through our network or stored on laptops, computers, other electronic devices, or our file servers.
- All computers, iPads, cell phones, or any mobile devices that need access to the school's computer network will be required to have a network management software client/agent installed on them. (This applies to all school-owned, laptop program, and personally owned devices.) This network client/agent software reports back to our network management system to verify user authenticity and device compliance. The network management system will also be used to manage assets, deploy software and policy updates, and ensure overall network compliance for all users. A device may not be able to gain access to the school's computer network without this client/agent software installed.

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.
- No file sharing or torrenting software of any kind is to be installed on school computers, including laptops or other electronic devices. Although these types of programs are software downloads, they automatically create file-sharing connections.

Software Installation and Downloading (All installation of software for the lower school will be done by the Technology Team.)

- Care should be taken regarding the loading of additional software. Viruses could be transmitted in this manner.
- All installed software must be a legally licensed copy of that software.
- The downloading and/or streaming of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
- The school reserves the right to remove any software that impedes academics.
- Movies subject to copyright protection may not be "ripped" from DVDs and placed on the laptops or desktops nor may copyright movies be downloaded to the laptops from the Internet unless there is specific permission to do so from the publisher. Only commercial videos and movies (such as television programs) legally purchased from the iTunes music store or another like entity may be downloaded to the laptops.

Shareware and Freeware

- The installation of shareware or freeware on school computers must have prior approval by a member of the Technology Department.
- Examples of such shareware and freeware programs include animated cursors (*e.g.*, Comet Cursor), screen savers, and others that may automatically open connections to the computers from the outside of our network. Those connections are made through spyware, and they monitor the activities on that computer as well as slow down the operation of the computer and the network connection.

Internet Use

- The Internet is a rich and valuable source of information for education. Inappropriate materials are available on the Internet, but 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.

- If a student accidentally accesses a website or other materials that contain obscene, pornographic, or otherwise offensive material, the student is to immediately exit the site and notify a teacher, an administrator, or a member of the technology staff so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.
- Information obtained through the Internet must be properly cited and in compliance with copyright laws. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized, when required by the instructor. 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.

Privacy, Use, and Safety

- Students are not to share any passwords or programs with any other student without specific permission from a faculty or staff member.
- Students are not permitted to communicate with or make plans to meet in person any person whom the student has contacted online.
- 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.
- 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 computers, email, and all other accounts. At no time, should initial default passwords be used. This is important in order to protect the privacy of each student.
- Students should use only assigned accounts. They should access other person’s files, accounts, records, or data only with permission from the owner.
- If inappropriate use of school email accounts and/or stored files by a student or employee including honor code violations or harassment is suspected, the school administration has the right to view these files in order to investigate suspected inappropriate behavior.
- The school may monitor computer activities that take place on campus during the school day 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 command prompt 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 computers.
- Students are prohibited from utilizing peer-to-peer networking or any method of file sharing between computers unless authorized by the technology staff.
- Students are prohibited from using computers or any electronic device laptops or any computer for acts of harassment or bullying cruelty (including email, blogging, text messaging, social media, etc.). Communication should be kind, courteous, and respectful.
- Students are prohibited from creating or accessing anonymous accounts or accounts created with a fake identity, especially if those accounts are used as a tool to bully, harass, or be unkind to others.
- Students are prohibited from using any type of app that creates anonymity for the user.
- Students are prohibited from disclosing confidential or proprietary information related to the school, making public remarks that defame or disparage the school, its employees, its students or its interests, or that recklessly disregards or distorts the truth of the matters commented on.

- IMPORTANT NOTE: Any laptop, mobile device, or wearable technology device used on the school network or school campus, even if privately owned, is subject to all policies and consequences of the Responsible Use Policy, including the right to view the content of the laptop or mobile device at any time, the right to remove content from that laptop or mobile device, and the right to retain the laptop or mobile device in the school's possession if there is an infraction to the RUP that deserves that consequence.

Copyright and Integrity of Data, Hardware, and Software

- Unauthorized duplication, installation, transmission, alteration, or destruction of data programs, hardware, or software is prohibited.
- Students must abide by licensing agreements and copyright laws.
- Games, music, software, movies, and pictures should only be obtained through legal means.
- Stripping or downloading audio or video files from YouTube or other online media sources is copyright infringement and therefore prohibited unless it is specifically in that site's terms of service.

Reporting Violations

- Students are expected to assist in the enforcement of this policy. If a student suspects a violation of this policy, or if a student feels nervous or uncomfortable about another school community member's use of technology, the student should immediately report the student's suspicions, feelings and observations to their Division Director.

Consequences

- The school reserves the right to enforce appropriate consequences for the violation of any section of the Responsible Use Policy for all students. Such consequences could include the loss of administrative privileges on a laptop, 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. These consequences apply to all students using laptops on the school's campus, whether those laptops are personally owned or issued by the school.
- School–issued computers with illegal or inappropriate software or materials on them will be reformatted or "re–-imaged," and the student may 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 laptop abuse and/or damages, the school has the right to revoke a student's privilege of using a laptop on campus.
- Laptop damage that is the result of intentional damage or negligence is not covered by insurance, and serious consequences will be incurred. This includes damage done to school–owned computers, loaner laptops, iPads, and other technology devices.
- If a student uses a cell phone or other electronic device during the academic day without permission from a faculty or staff member, the device will be collected and sent to the appropriate administrator's office. Consequences will be discussed when the cell phone or other device is returned to the student. A student who accumulates several of these violations may lose the privilege to carry the device on campus.
- Students are to report any known violations of this Responsible Use Policy to appropriate teachers, administrators, or technology staff members. Random checks of student laptops (both personally owned laptops and school-issued laptops) will be conducted throughout the school year to ensure that these policies are being followed.

Students are required to adhere to all provisions and conditions set forth in this Responsible Use Policy. Any violations of this policy will result in disciplinary action, the loss of laptop privileges, and possible legal action. Students are to report any known violations of this Responsible Use Policy to appropriate teachers, administrators, technology staff members or the Honor Council. St. George's Independent School takes no responsibility for activities conducted on school computers and laptops, personally–owned or school–issued laptops, and electronic devices or materials stored on such computers, laptops, or the school's network. The Responsible Use Policy is current as it resides on the St. George's website and will be updated to include any additions or corrections.

RESPONSIBLE USE POLICIES FOR
TECHNOLOGY AND ELECTRONIC DEVICES
ST. GEORGE'S INDEPENDENT SCHOOL

2016-2017

Students are required to adhere to all provisions and conditions set forth in this Responsible Use Policy. Any violations of this policy will result in disciplinary action, the loss of laptop privileges, and possible legal action. Students are to report any known violations of this Responsible Use Policy to appropriate administrative staff members or the Honor Council. St. George's Independent School takes no responsibility for activities conducted on school computers and laptops or materials stored on computers, laptops, or the network.

IMPORTANT NOTE: *Any laptop or mobile device (including cell phones and wearable technology devices) used on the school network or school campus, even if privately owned, is subject to all policies and consequences of the Responsible Use Policy, including the right to view the content of the laptop or other mobile device at any time, the right to remove content from that laptop or mobile device, and the right to retain the laptop or mobile device in the school's possession if there is an infraction to the RUP that deserves that consequence.*

I agree to abide by the guidelines of the Responsible Use Policy as described above. I understand that there will be consequences for not adhering to these guidelines. These could include the loss of laptop privileges for serious infractions.

Grade ______________

Student Name ____

____

Student's Signature

____

Parent's Signature