Acceptable Use Policy (AUP) 2018-19

The goal of the Acceptable Use Policy is to provide a full range of technology tools, services and experiences to support the school's mission statement. Each STA graduate should possess skill in using a wide variety of technology; they also should develop habits that ensure their use of technology is efficient, respectful, legal and safe.

Technology is an ever changing component to the twenty-first century learner. Therefore, STA reserves the right to amend or revoke the policy and/or procedures in this technology agreement at any time as circumstances may require. STA students will be required to read and abide by these standards each year.

Under this policy, parents are responsible for monitoring their daughter's use and care of the tablet during off school hours.

Part 1: Network ID's Passwords and Security

Each student will be issued her own password to access school computers, their issued tablet, PowerSchool, Email and other services. It is the responsibility of the student to ensure the confidentiality of her own password. Individuals will be held responsible for the information stored and/or transmitted via their account or equipment, even if it resulted from someone else who was given access.

Faculty, Staff and School Administration have the right to request access to a student's tablet at any time. Students are responsible for keeping their tablet safe and should not allow anyone else, including fellow students, to access their tablet. To protect the integrity of a computer system involving many users, STA students must follow these guidelines:
- **DO NOT** reveal their password to another user.
- **DO NOT** use another student's password to gain access to services.
- **DO NOT** use another student's tablet.

Network security applications are on each school device and are updated regularly by STA. It is a violation of policy for a student to delete or disable these applications. Individuals are prohibited from any action that will compromise the privacy and/or security of others.

The school reserves the right to access any file, network transmission or other information stored on and/or communicated through its property at any time and for any reason, including random access to check on compliance with this policy. All storage, network communication, equipment and software provided by STA shall remain the property of STA.

STA email accounts that are provided to all students are not private email accounts and can be accessed by administration at any time. All email activity, for any school issued email account, is logged and archived.

Part 2: Printer Usage

Students will not intentionally waste limited resources such as paper provided by STA. Only school-related materials should be printed with school resources. All students will be allocated $10 per student printer. Full pricing details are available in the student handbook.

Part 3: Photography & Recording (Camera & Mic)

St. Teresa's Academy wishes to avoid any impropriety, harassment or photography in inappropriate situations that may be associated with the use of any camera devices. This is especially true in places where students, faculty, staff and visitors have an expectation of privacy, such as bathrooms, locker rooms, dressing areas, etc. Devices may not be used and must be turned off in areas of privacy.

Student tablets are equipped with the ability to record audio and video. At no time should a student record anyone (student, teacher, parent, presenter, etc.) without permission from the parties involved. The use of cameras on phones or other audio or video recording-capable devices on the campus of St Teresa's Academy may constitute an invasion of personal privacy. The use of a camera or other audio or video recording-capable devices on St. Teresa's premises is prohibited without the express prior permission of the person(s) present at the time.

Inappropriate use of phones, cameras, and electronic tablets may result in corrective action including detention or suspension.

Part 4: Network, Internet Access, Monitoring & Filtering

Internet communications on, and off, campus are monitored and filtered. Our goal is not ultimately to restrict student access, but to educate students about responsible and appropriate use. Students using the Internet are representatives of the school and are expected to act in a manner consistent with the school's goals and values. Communications on the Internet reflect on STA and must not damage the school's reputation.

The Internet is to be accessed for scholarly research and/or means of obtaining needed educational information only. Students are prohibited from using the Internet for any other purposes during the school day. Use for commercial activities, product advertisement or political lobbying is also prohibited. This prohibition includes, but is not limited to, copyrighted materials, threatening or obscene materials, or material protected by trade secret. The student takes responsibility for all content found on the tablet. Consequences include confiscation of the student's tablet and may include but not limited to: detention, Student Behavior Report, suspension, student expulsion and referral to law enforcement authorities.

STA reserves the right to monitor device and activity usage of all students. STA incorporates both a network-based and a client-side content-control system. Students are not allowed to access any inappropriate web site. If a student has reason to believe that an inappropriate site has been blocked they may contact the Help Desk or submit the site for review.

Students may not use any chat, collaboration program or other services (such as Moodle) to communicate with others during class, unless a teacher or administrator authorizes students to do so. The playing of games during class time, without teacher approval, is also prohibited. Students may not download programs or games without administration approval.

Students are subject to random security and usage checks on any school service or device. Administrative decisions regarding unacceptable service or device usage may result in the student's use to be revoked, denied or suspended. All administrative decisions will be final.

If students create and share web pages, such as a wiki-space, or anything on a cloud storage service (such as Google Drive) for an assignment, the share must be approved by the teacher and must be accessible only to members in that specific class, unless given permission by the teacher or administrator for broader access. Using the school name, logo and images is prohibited unless authorized by administration.

Students will disclose to an administrator or teacher any message they receive that is inappropriate or discomforting, be it on social media, SMS or other messaging apps. Staff, students and others involved in school activities have the responsibility to report to the administration any threats of violence or harm, hate, and/or incidents of bias. Depending on the significance and credibility of the threat, it will be reported to law enforcement.
- **DO NOT** make comments that could be misconstrued, as electronic text allows no context clues to convey shades of irony, sarcasm or harmless humor.
- **DO NOT** knowingly or recklessly post false or defamatory information about another student or STA.
- **DO** notify the Help Desk immediately if you mistakenly access inappropriate information. This will protect against a claim that they have intentionally violated this policy.

Plagiarism is defined as taking ideas or writings of others and presenting them as if they were your own.

- **DO NOT** plagiarize works from any source, including those found on the Internet, in electronic databases or other online research tools.
- **DO** cite, following the citation format, such as MLA, set by the teacher, in all works that are not original to that student.
- **DO NOT** plagiarize another student's work, such as sharing school-related files when the project, activity or assignment is to be done independently.

Part 5: Social Media

St. Teresa's Academy recognizes that there are legitimate academic, and personal, reasons for using social media at school or using school computing resources. To enable students to take advantage of the values of these sites and to promote an open, trusting and collaborative learning environment, our policy allows students to use social media within the guidelines specified below. St. Teresa's Academy does have the ability to monitor and record social media activity as per our filtering guidelines. For the privacy of users and their families, please assume that all postings to STA-sponsored sites will be publicly available on the Internet and therefore publicly accessible without limitation or protection of any kind.

What is Social Media?

Social media refers to forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos or pictures). Examples of such destinations include large branded entities such as Facebook, Twitter, YouTube, Instagram, Snapchat and LinkedIn. However, blogs, special interest forums and user communities are also considered social media.

Inappropriate Content

While social media contains legitimate content, they also include content that is inappropriate for school including nudity, violence, hate, incidents of bias, abused drugs, sex and gambling. Therefore, the same inappropriate content policy that applies to the broader Web, also applies to content found within social media. Inappropriate content should not be accessed by students on school issued devices or devices connected to the school network. Students should use common sense and consideration for others in deciding which content is appropriate.

Content Publishing and Confidentiality

The following are policy guidelines regarding what you should and should not do when publishing content in social media. These guidelines apply to all social media communications whether personal or school-sponsored. Students are responsible for content they publish in social media and can be held personally liable for content published. Students also can be subject to disciplinary action for publishing inappropriate or confidential content. These guidelines only cover a sample of all possible content publishing scenarios and are not a substitute for good judgement.

- **DO** know and follow all privacy and confidentiality guidelines as noted in Part One of this document. All guidelines in the student handbook, as well as laws such as copyright, fair use and financial disclosure laws apply to social media.
- **DO NOT** disclose any personal contact information about yourself or others. Personal contact information includes, but is not limited to, home addresses, telephone numbers, parental and/or guardian names. Students agree not to meet with any individual they have communicated with online.
- **DO NOT** disclose or use St. Teresa's Academy confidential or proprietary information or that of any other person or company. For example, ask permission before posting someone's picture in a social network or publishing in a blog a conversation that was meant to be private.
- **DO NOT** cite or reference other students, faculty, staff, administration or partners without their written approval.
- **DO** identify yourself. Some individuals post anonymously, using pseudonyms or false screen names. St. Teresa's Academy discourages that practice.
- **DO** be professional. If you have identified yourself as a St. Teresa's Academy student within a social website, you are connected to the faculty, staff, administration and even fellow students.
- **DO** ask for permission to publish or report on conversations that are meant to be private or internal to St. Teresa's Academy and when in doubt, always ask permission from the administration.
- **DO** speak in the first person when engaging in personal social media communications. Make it clear that you are speaking for yourself and not on behalf of St. Teresa's Academy.
- **DO** link back to the source when you do make a reference to a faculty, staff, student or school partner where possible.
- **DO** be aware of your association with St. Teresa's Academy social media. If you identify yourself as a St. Teresa's Academy student, ensure your profile and related content is consistent with how you wish to present yourself with faculty, staff, administration and fellow students.

- **DO** use your best judgment - Remember that there are always consequences to what you publish. If you're about to publish something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you're still unsure, and it is related to St. Teresa's Academy, feel free to discuss it with administration or simply do not publish it. You have the sole responsibility for what you publish in any form of social media.
- **DO NOT** use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in the school environment. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.
- **DO NOT** register accounts using the St. Teresa's Academy name or any other unregistered or registered trademarks.
- **DO NOT** engage in demeaning behavior, including harassment, bullying, hazing, name calling, acts of hate, incidents of bias and threatening of another person. Harassment is persistently acting in a manner that distresses or annoys another person.
- **DO** be aware that your digital footprint follows you to college and on through employment.
- **DO NOT** assume that because something has been deleted, it can't be retrieved or wasn't captured in a screenshot by another party.

User agrees to indemnify and hold harmless St. Teresa's Academy, its affiliates, directors, employees, administration and assigns against any damages, losses, liabilities, judgments, causes of action, costs or expenses (including reasonable attorneys' fees and costs) arising out of any claim by a third party relating to any material user has posted on STA-sponsored sites.

Online Crime Prevention

Social media is commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal confidential information. To minimize risk related to such threats, adhere for the following guidelines. While these guidelines help to reduce risk, they do not cover all possible threats and are not a substitute for good judgment.

- Do not use the same passwords for social media that you use to access school resources.
- Do not follow links or download software on social media pages posted by individuals or organizations that you do not know.
- If any content you find on any social media web page looks suspicious in any way, close your browser and do not return to that page.
- Configure social media accounts to encrypt sessions whenever possible. Facebook, Twitter and others support encryption as an option. This is extremely important for roaming students who connect via public Wi-Fi networks.

Part 6: Help Desk

A Technology Help Desk is located in the Goppert Building. The service desk is provided during school hours to help students with technical problems. A student must seek help as soon as a computer problem surfaces. Unresolved problems can magnify support issues and cause other problems to occur. Students are expected to be active participants in problem resolution.

Students needing technical assistance may seek it before or after school, during lunch/activity or unstructured time in their schedules.

If a tablet is left at the Technology Help Desk for repair, a loaner will be issued and all policies set forth in this AUP shall apply to the loaner. Students will be notified when their tablet repairs are complete. If a tablet repair has been completed but the student has not picked it up from the Help Desk, this will not be an acceptable excuse for the failure to turn in work and/or complete a classroom assignment. Students will be billed for loaned items not returned to the school.

Part 7: Tablet Care, Protection and Responsibilities:

The tablet that students receive actually belongs to St. Teresa's Academy, and is very expensive. The tablet is yours for this school year and is to be used for academic purposes, both on and off campus. You have the responsibility of taking good care of it.

Should any student experience a problem with their tablet case (i.e., faulty strap or zipper) or tablet then they must report the problem to the Technology Help Desk as soon as possible.

- **DO** keep the tablet away from foods and drinks and only use the touch screen with clean hands.
- **DO** keep your tablet in the school provided case at all times, when not in use.
- **DO** carry your tablet with both hands (not one) with the lid closed and the case zipped.

- **DO** use your tablet only on a stable surface (i.e. do not balance it on your lap).
- **DO NOT** carry your tablet inside of a backpack.
- **DO NOT** alter your tablet, or case, in any way (i.e. stickers, writing).
- **DO NOT** leave your tablet, in or out of the case, on the floor where it could be stepped on. Cases must be put under a desk or hung on the back of a chair when not used during class time.
- **DO** charge your tablet nightly. Students will not be able to claim a forgotten or uncharged tablet as an excuse for failed or incomplete assignments.
- **DO** bring your charger with you each day.
- **DO** be courteous and mute the tablets audio when using it at school.
- **DO NOT** intentionally destroy the integrity of computer-based information.
- **DO NOT** install malicious programs, invoke a computer virus or any other disruptive mechanism.
- **DO NOT** alter system files or configuration to disrupt computer or network functions.
- **DO NOT** seek or gain unauthorized access to network resources on the Internet or attempt to breach security mechanisms.

Students are responsible for backing up any critical files on a regular basis to a flash-drive or cloud storage service. Tablet malfunctions are not an acceptable excuses for failure to turn in work. Help Desk technicians are not responsible for the backing up of files if the computer is brought in for repair.

Tablets may not be used in the Commons during lunch periods. Tablets should not be put in situations that increase the risk of theft or incidental damage. Tablets and chargers must never be loaned to someone or left unattended/unsecured. During the school day, students must have their tablets with them at all times or locked in their school locker. **Tablets should go home with students each evening and must not be left in their car for an extended period of time.** The use of stickers, paint or markers on the tablet is prohibited. If a student leaves STA then the tablet, pen device, charger and STA provided case must be returned upon withdrawal.

A student may lose tablet privileges and administration reserves the right to make all final decisions.

Part 8: Liability

Insurance is provided by the school for all school issued tablets. This insurance covers theft & vandalism (police report required), accidental damage (such as drops/cracked screens/liquid spills), natural disasters, power surges due to lightning and fire/flood damages. All insurance claims must be made through the Help Desk.

Please Note: The insurance above only applies to the tablet and not to the keyboard, protective case, bag, pen or charger.

STA will provide replacements for any mechanical defect that is not a direct cause of misuse. Examples of such defects include, but are not limited to, a bad hard drive, pen stops functioning, charger stops charging or the keyboard no longer works.

Damage due to negligence, carelessness or misuse (even if covered by the insurance) may result in disciplinary consequences, as well as monetary consequences, as determined by the administration.

Part 9: Consequences and Due Process:

The use of the tablet is a privilege. A student whose behavior or repair record indicates careless use or abuse of her tablet or other technical resources will be referred to the administration for appropriate disciplinary action.

The administration has the right to restrict or terminate network and Internet access at any time to protect the integrity of the network or prevent misuse.

The administration will notify parents/guardians of any violation of the agreement and the nature of the violation. Upon request, parents may view any materials or printouts related to the violation, although the administration reserves the right to send material home without the request of the parents as well. The purpose of parental review is intended to be a tool to inform parents/guardians and to assist them in guidance of their daughter, not an appeal process.

Any student whose tablet has been confiscated for any violation will not be allowed to borrow a school loaner nor use another student's tablet. Violation(s) of the AUP include but are not limited to: detention, Student Behavior Report (SBR), suspension or revocation of computing privileges and other technological privileges, suspension, expulsion from school, legal action (including action to recover damages or cost of the computer) and referral to law enforcement authorities.