Technology Acceptable Use Policy - 2019-2020 School Year
3/12/2020 Revisions in Red

I. Purposes and Use Expectations for Technology

A. **St. Michael the Archangel Catholic School offers a robust technology program, to provide and support rigorous instruction for all students.**

B. **Devices primarily stay on the school campus. However, in the event that school devices are sent home with students, the policies, expectations, and spirit contained within this document remain.**

1. Individual devices owned by StMS are the property of the school. All personal customization of these devices is prohibited, including but not limited to the altering of settings within the device or changing background images within a browser page.

C. **The use of all school-owned technologies, including the school network and its Internet connection, is limited to educational purposes for students and student visitors of St. Michael School.**

1. The network is provided for student instruction, to conduct research, and create reports, projects or presentations. Access to network services will be provided only to those students who agree to act in a considerate and responsible manner.
2. This access is a **privilege**- not a right. This privilege comes with personal responsibilities and violation of the responsible use of any school technologies may result in the **privilege** being revoked and/or suspended.
3. Students will review yearly rules and procedures for proper use of school owned technology, including the school network and acceptable and unacceptable uses, annually. In addition, students and their parent or guardian must sign the Handbook's Parent and Student Signature Page each year in order to acknowledge the StMS Technology Acceptable Use Policy before using school technologies at the start of each new school year.

D. **St. Michael Catholic School adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act.**

1. All access to the Internet is filtered and monitored. The school cannot monitor every activity, but retains the right to monitor activities that utilize school owned technology and interactions that take place online or through the use of technology on our property or at our events.
2. While the teachers and staff of StMS will make a concerted effort to control student access to this material and maintain a filtering system, StMS cannot control the content of material available on the Internet or user access to that material. St.

Michael School also reserves the right to investigate any reports of inappropriate actions related to any technology used at school.

E. **Students will be supervised by teachers at all times and expected to act responsibly and thoughtfully when using technology.**
   1. Students can only use school and personally owned technology during an appropriate technology class or under direct supervision by a teacher for a technology oriented lesson in designated areas only.
   2. Students are responsible to inquire with the supervising adult when they are unsure of the particular use of technology prior to engaging in the use. During school, teachers will guide students toward appropriate educational material. However, it will be the responsibility of the student to not pursue material StMS considers offensive.
   3. Student activity is monitored by teachers using Go Guardian, an online security program, whether on campus or at home.

II. School Resources

A. Technology is a finite, shared resource offered by the school to its students. This technology includes hardware, software, and campus-wide Internet/network access. File storage areas will be treated like lockers or any other storage area on campus. Users should not expect that files stored on the school network or school property will always remain private. School and network administrators may review profiles to maintain system integrity and ensure that users are using the system appropriately. Students will be expected to respect the password protection and privacy of all network users. Students are responsible for keeping the device clean and the battery charged, whether devices are at school or at home.

B. St. Michael School has wireless Internet that is protected by a password. Unauthorized access is not allowed. If an individual desires to connect a laptop or a personal technology device (PTD) to the Internet under the direct supervision of a teacher during a lesson, please contact a member of the Technology staff.

C. The school provides individual technology accounts for students to keep track of their technology use. Users must log off when they are finished using a school computer. Students are responsible for any activity that occurs through their personal account.
   1. Programs used at St. Michael School for individual student accounts include, but are not limited to: Google Drive®, RenWeb®, Pearson Math® and Wonders®.
   2. Students will review rules and procedures for using these school programs annually, with the assigned homeroom teacher at the start of each school year including acknowledgment of the StMS Google Drive Agreement (Appendix A).

D. Upon graduation or student transfer from St. Michael School, access will no longer be granted to the school network, the interactive data management system, the StMS Google Drive account, or files stored on the school network. Prior to graduation, we recommend saving all personal data stored on school technology to a removable hard drive.

III. Unacceptable Uses of Technology

No policy can detail all possible examples of unacceptable behavior related to technology use. School technology users are expected to understand that the same rules, guidelines, and policies that apply to non-technology related student behavior also apply to technology-related student behavior. School technology

users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet. Any improper use of technology off campus is also subject to disciplinary action. If there is ever an uncertainty regarding acceptable use, ask the teacher or Administration for assistance.

A. Respect for the Privacy of Others and Personal Safety
    1. St. Michael School is a community and as such, community members must respect the privacy of others. The following items are some examples of inappropriate usage:
        - Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others.
        - Do not misrepresent or assume the identity of others.
        - Do not re-post information that was sent to a student privately without the permission of the person who sent the information.
        - Do not post private information about another person.
        - Do not use another person's account.
        - Do not use any accounts outside of the terms of which access to that account was given.

    2. Do not voluntarily post private information about yourself online, including your name, your age, your school name, your address, your phone number, or other identifying information.

    3. St. Michael School prides itself on its reputation for excellence; therefore, students and parents may not use the school's name, logo, mascot or other likeness or representation on a non-school website without express permission from our school.

B. Academic Honesty, Personal Integrity, and Plagiarism
    1. All students are expected to maintain academic honesty. Do not claim or imply that someone else's work, image, text, music, or video is your own. This is plagiarism and will not be tolerated. Plagiarism is also when you incorporate a piece of someone else's work into your own without giving appropriate credit. Do not pretend to be someone else online or use someone else's identity.

    2. Songs, videos, pictures, images, and documents can all be copyrighted. Make sure to appropriately cite all materials used in your work. Students may not utilize someone else's work without proper permission.

C. Computer Settings and Computer Labs
    1. Students are not allowed to alter, change, modify, repair, or reconfigure settings, including but not limited to desktop backgrounds or themes, on school-owned computers or programs without the express prior permission of the Technology Department. Students may not download any programs, applications, or extensions to any school-owned device.

    2. Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.

    3. Food and drink are prohibited from school computer labs. Students may not eat or drink while using any school-owned computers, devices, or other technologies.

4. Students may not circumvent any system security measures. The use of websites or hot spots to tunnel around firewalls and filtering software is expressly prohibited. The use of websites to hide the user's identity is prohibited. The use of websites to circumvent any school policy is prohibited. Students may not alter the settings on a computer in such a way that the virus protection software would be disabled. Students are not to try to guess passwords. Students are not to access any secured files, resources, or administrative areas of the school network.

D. Communication: Instant Messaging, Email, Blogs, Social Media, etc.

1. Students are not permitted access through any school-owned technologies to any personal accounts, blogs, or other social media services including, but not limited to, the following: Facebook®, Twitter®, Skype®, Yahoo! Messenger®, Gmail®, Gtalk®, Instagram®, Snapchat®, Vine®, etc.

2. Engagement in the online blogs and/or social media platforms may result in disciplinary actions if the content of the student's blog, or a parent's blog, includes defamatory and/or negative comments regarding the school, faculty, staff, other students, and/or the parish.

3. Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students. If told by another person to stop sending such communications, it must stop immediately.

4. Inappropriate communication includes, but is not limited to, the following:
    a) profane, sexual, vulgar, rude, inflammatory, threatening, or disrespectful language or images taken, typed, texted, posted, or spoken by students and/or about other students.
    b) information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment
    c) personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others
    d) knowingly or recklessly posting false or defamatory information about a person or organization, including St. Michael School
    e) communication that promotes the destruction of property, including the acquisition of destructive devices.
    f) technology use intended to harass, demean, humiliate, intimidate, or annoy their classmates or others in the StMS community. This unacceptable student behavior is cyber-bullying and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to disrupt the safety or well-being of the school is subject to disciplinary action.

    Students involved in the possession or transmission of inappropriate material, whether on one's phone or other electronic device, face suspension and/or expulsion.

E. Social Networking and Website Usage

1. Students may have social networking profiles or accounts, but are not permitted to access social media sites through school owned technology, nor on their own device while on school property using the school network.

2. Students may not use virtual reality sites in order to create avatars that depict students, teachers, or staff in a defamatory light. Parents are cautioned to be aware of such online sites visited by their children, knowing that often predators are not living in a neighborhood, but within the home via a computer.

3. Students may not access any online material that is offensive, profane, or in any way contrary to the vision, mission, and values of our Catholic identity.

F. Cell Phones and Personal Technology Devices (PTD)

1. Cell phones and/or personal technology devices (PTD) are not to be used for texting, accessing the Internet, streaming data, and/or making videos or calls between 7 a.m. and 3:30 pm, or if attending the After School Care Program or school sponsored after school activities, unless students have explicit permission from the supervising teacher for educational purposes. Devices must be powered OFF - not merely silent or on vibrate - and stored in one's locker; if a device is needed for educational purposes or is needed after school hours, device must remain powered OFF and properly stored until the supervising teacher grants permission to retrieve the PTD for the relevant activity.

2. It is the student's responsibility to adhere to all acceptable use policies in order to maintain the privilege of having a cell phone or PTD at school or at school events.

G. Recording, Video, and Photography

1. Students are not permitted to send or take photographs or video with their phones on school property or at school events without permission from the supervising teacher.

2. School devices with built-in cameras or videos may only be used for teacher-directed educational purposes. Students are not permitted to take photographs or video with any school-owned device without permission from the supervising teacher for an educational purpose.

H. Downloads and File Sharing

1. Students may never download, add, or install new programs, software, or hardware onto school-owned devices. Downloading sound and video files onto school-owned computers is prohibited.

2. Students may never configure school devises or personally owned computers to engage in illegal file sharing. Students who engage in illegal file sharing may face disciplinary action.

I. Commercial Use

1. Students may not use school technology to sell, purchase, or barter any products or services.

IV. Personal Technology Devices

A. All personal technology devices (PTDs) may not be used during regular school hours or during school sponsored activities, including after school activities, unless otherwise allowed by the supervising teacher for educational purposes.

B. Devices capable of capturing, transmitting, or storing images or recordings may never be accessed, turned on, or operated in areas where there is a reasonable expectation of privacy.

C. To protect the safety and well-being of the StMS community and in order to avoid disruption to the learning environment, the StMS faculty and staff reserve the right to confiscate any PTDs. Confiscated cell phones and PTDs, which includes smartphones, iPads®, iPods®, MP3 Players, gaming devices, Apple Watches®, Smart Watches, or watches for texting or communicating, will remain in the Principal's or Assistant Principal's office until the student's parent can retrieve it in person.

D. The content of the device may be reviewed as part of any investigation of policy violation or other inappropriate use. Appropriate actions will be taken, up to and including the notification of local authorities if necessary. St. Michael School is not responsible for any damage or harm to the PTD, including but not limited to loss, theft, damage, or destruction of PTDs or any of their contents.

V. Summary

A. The school Administration shall have broad authority to interpret and apply these policies. Restrictions may be placed on the access of school technologies, or privileges may be revoked entirely, should an infraction occur against the Technology Acceptable Use Policy. Additional disciplinary measures may also occur.

B. If inappropriate information is accidentally accessed or received, the supervising teacher or Administration should be notified as soon as possible.

C. If deliberate or accidental access to inappropriate information or technology use is witnessed, individuals must report the incident to the supervising teacher or Administration as soon as possible.

D. The school retains the right to suspend service, accounts, and access to data, including student files on school accounts such as Google Drive®, if the integrity of the school network is compromised.

E. Since technology is continually evolving, St. Michael School reserves the right to change, update, and edit the StMS Technology Acceptable Use Policy at any time in order to continually protect the safety and well-being of our students and community. To this end, the school may add additional rules, restrictions, and guidelines at any time.

VI. School Accountability

A. The school cannot and does not guarantee that the functions and services provided by and through technology will be problem-free. The school is not responsible for any damages students may suffer, including but not limited to, loss of data or interruptions of service. The school is not responsible for the accuracy or the quality of the information obtained through school technologies. Although the school filters content obtained through school technologies, the school is not responsible for student's exposure to "unacceptable" information, nor is the school responsible for misinformation.

VII. General Safety and Security Tips for Use of Technology

A. Communications: All forms of communication, including emails, videos, text messages, Snapchat®, etc., may not be retrievable once it is sent out. However, those who receive it may make it public or send it along to others, despite one's intentions.
B. Passwords: Do not share passwords with friends. When creating a password, remember to include both capital and lowercase letters, as well as numbers in your password if possible.

VIII. Definitions and Terms

A. Cyber-Bullying: A person is cyber bullied when he or she is exposed online to negative actions on the part of one or more persons, and that person has difficulty defending himself or herself. An example of cyber-bullying includes when someone sends derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyber-bullying also takes place when someone purposely excludes someone else online.

B. Technology: Under this policy, technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, digital media players, gaming devices, cell phones, CDs, DVDs, calculators, scanners, printers, cameras, hard drives, USB drives, modems, servers, wireless cards, routers, the wireless network, and the Internet. School technology refers to all technology owned and/or operated by the school.

C. Personally Owned Device User: Personally owned device user refers to anyone who utilizes their own personal technology device (PTD) on campus, at a school-sponsored event, or while accessing St. Michael School's wireless network. In this case, individuals are still subject to the StMS Technology Acceptable Use Policy.

**This policy was created from a Campus Outreach Services© policy resource. For information on utilizing any language in this policy, please contact COS directly.*

StMS Google Drive Agreement

Appendix A

Google Drive is an online program which will provide students and teachers with the ability to work on documents, spreadsheets, and presentations from any computer with Internet access. Students will use Google Drive and its features in order to best complete school work at St. Michael the Archangel Catholic School.

However with new technologies, there are lessons to be learned. Instructions regarding procedures for proper and appropriate use of Google Drive, as well as guidelines to maintain safety for all users, will be reviewed with the assigned homeroom teacher at the start of each school year. Before students will be granted access to a StMS Google Drive account, they are required to read the following information and review annually as a part of the Parent/Student Handbook, and acknowledge the introduction and instruction of the proper use of Google Drive, as well as agree to follow all guidelines for using a St. Michael School Google Drive account.

- I understand Google Drive will be considered a part of the technology program at StMS. Therefore, the rules that apply to all students in the StMS Technology Acceptable Use Policy in the Parent/Student Handbook will also apply to Google Drive.
- I understand the StMS Google Account access is considered property of St. Michael Catholic School, and any work done through the school Google Account, whether on or off-campus, is subject to the StMS Technology Acceptable Use Policy.
- I understand there are rules to be followed when using StMS Google Drive. Access to a StMS Google Drive account is a privilege, not a right, and inappropriate use may result in the elimination of these privileges.
- I understand documents and other works may be shared with teachers, administrators, and peers through StMS Google Drive. This will allow students the opportunity to "submit" work without printing. Students are to follow the directions for sharing as instructed by the supervising teacher. Any time work is to be shared among students, it will be for educational purposes only, such as for a cooperative learning activity, group project, or peer editing.
- I understand any violations of this agreement will be subject to the StMS Technology Acceptable Use Policy in the Parent/Student Handbook.