

Saint Michael Catholic School Technology Handbook for Students and Parents

Student Computing Goals

1. Improved Student Learning
2. Meaningful Student Engagement
3. 21st Century Skills
4. Project and Problem-based Learning Opportunities
5. Equity of Access

Responsible Use Procedures (RUP)

When signing the Responsible Use Procedures, you are acknowledging that you understand and accept the information in this document and agree to Saint Michael Catholic School (SMCS) Responsible Use Procedures and Terms and Conditions for Device Usage.

Saint Michael Catholic School students and families must understand that:

1. Devices are available for student use and remain the property of Saint Michael Catholic School.
2. All users are accountable to all school, local, state, and federal laws.
3. All use of devices and network must support education.
4. Students and families must follow all guidelines set forth in this document and by SMCS staff.
5. All rules and guidelines are in effect before, during, and after school hours, for all SMCS devices whether on or off the school campus.
6. All files stored on SMCS equipment are the property of the school and may be subject to review and monitoring at any time.
7. The term “equipment” or “technology” refers to devices, batteries, power cord/chargers, and cases. Each piece of equipment is issued as an educational resource. The conditions surrounding this equipment can be equated to those of a textbook.
8. Students are expected to keep the devices in good condition.
9. Students are expected to report any damage to their device as soon as possible to their teacher. This means no later than the next school day.
10. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.
11. Students are expected to notify a staff member immediately if they come across information, images, or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
12. All users are expected to follow existing copyright laws and educational fair use policies.
13. Students may only log in under their assigned username. Students may not share their password with other students.
14. Students should not loan device components (i.e. chargers) to other students. Students who do so are responsible for any lost components.
15. Any failure to comply may result in disciplinary action. SMCS may remove a user’s access to the network without notice at any time if the user is engaged in any unauthorized activity.
16. SMCS reserves the right to confiscate the property at any time.

Parent/Guardian Responsibilities

Saint Michael Catholic School makes every effort to equip parents/guardians with the necessary tools and information to ensure safe use of the devices in the home. There are several responsibilities assumed by the parent/guardian and the student. These are outlined below.

- All Parents/Guardians and Students are required to sign the Responsible Use Procedures.

Device Rules and Guidelines

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when they use a school-owned device. In general, this requires efficient, ethical, and legal utilization of all technology resources. Violations of these rules and guidelines will result in disciplinary action. Students will receive device-related training at school when they obtain their device.

- **All use of technology must:**
 - Support learning
 - Follow local, state, and federal laws
 - Be school appropriate
- **Security Reminders**
 - Do not share logins or passwords
 - *Exception: students should share passwords with parents or guardians*
 - Follow Internet safety guidelines
- **Students are prohibited from:**
 - Defacing SMCS issued equipment in any way. This includes but is not limited to marking, painting, drawing, adding stickers, or marring any surface of the devices or any stitching on the case.
 - If such action occurs, the student will be held responsible.

Caring for the Device

- The device is school property and all users will follow these procedures and the Saint Michael Catholic School Responsible Use Policy.
- Students should use the device assigned to them and not lend their device to others.
- Students are responsible for the general care of the device issued by the school.
- Students are responsible for keeping the device's battery charged for each school day.
- Students with a damaged device or a device failing to operate properly must notify a teacher or staff member.
- Only use a clean, soft cloth to clean the screen; no cleansers of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Devices must never be left unattended, in an unlocked car, unsupervised area, or in extreme temperatures.

Carrying the Device

- Devices assigned to students in 5th-8th grade must be in a carrying case anytime they are not in use.
- Carrying cases should not hold other objects. Folders, workbooks, etc. should be kept in a book bag or carried separately to avoid placing excessive pressure and weight on the device screen.
- Chromebooks and cases will have nametags and they should not be removed or altered in any way.

Carrying Case

- Students in grades 5 - 8 are assigned a device carrying case from Saint Michael Catholic School. Each student is expected to retain the case and device for the duration of their enrollment at Saint Michael Catholic School.
- Students are expected to protect and take proper care of their device carrying cases.
- In the event of a lost, stolen, or otherwise unusable carrying case, students must purchase the current school standard carry case from SMCS.

Screen Care

- Screen damage will occur when pressure is applied to the screen. Users must avoid closing anything in the Chromebook (i.e. pencils, crayons, etc.) and should not place anything on top of the Chromebook whether it is in or outside of the carrying case.
- The screen must be cleaned only with a dry soft cloth or anti-static cloth. No cleaners of any kind should be used on the device.
- The device must not be bumped against lockers, walls, car doors, floors, etc. as the screen can be broken.

Care of Device at Home

- Charge the device fully each night.
- Store the device on a desk or table - never on the floor!
- Protect the device from: Extreme heat or cold. - Food and drinks. - Small children. - Pets.
- Do not leave the device in a vehicle.
- In case of theft, an official police report will be required.

Technology Fee

- A yearly fee of \$120 is issued to insure the device.
- For students in grades 5-8, the technology fee must be paid for the chromebook to be taken home.

Repairs/Loaner Device

- If a student's device needs to be repaired, the technology coordinator will issue a loaner Chromebook for use at school. No loaner Chromebooks will be allowed to go home.

Email and Clever for Students

All Saint Michael Catholic School students are issued a school email account. Saint Michael Catholic School email allows students to safely and effectively communicate and collaborate with SMCS staff and classmates, giving them an authentic purpose for writing.

The use of Clever, an educational technology platform that allows students and teachers to access as many of their school-approved digital learning programs and resources as possible through one login, is being used this year to streamline access. It allows secure management and distribution of applications, online textbooks, etc.

Email Usage

- The primary purpose of the student electronic mail system is for students to communicate with school staff and fellow students to collaborate on school activities.
- Students are responsible for good behavior while using the school email (at school and at home), just as they are in a classroom or hallway.
- Access to email is given to students who agree to act in a considerate and respectable manner. Access is a privilege - not a right. Access entails responsibility.
- Students are responsible for messages sent from their accounts.
- Students should not share their passwords.
- Students should not give out personal information over email, including home telephone numbers or home addresses.
- Students will not use email to bully, harass, or threaten other students or individuals.
- Students will report any unusual activities such as "spam" communications to their teachers.
- Students will not use email to send chain letters, viruses, hoaxes, or forward social or non-school related email to other students or staff.

- Email accounts are filtered and messages written containing inappropriate language or content will be flagged and administration alerted.
- Student email is provided by the school and is school property. SMCS reserves the right to archive, monitor, and/or review all use of its email system, and users should not have any expectation of privacy in any electronic message created, sent, or received on the school's email system.
- Student email accounts will be removed from the system after middle school is completed, leaving the school, or disciplinary actions. If necessary, SMCS, at its discretion, may close the accounts at any time.

Email Etiquette

- **Please don't SHOUT!** If you type in all capital letters, your reader will see this as yelling. It's also hard on the eyes. Did you know that it takes longer to read something written in all caps than it does to read something that is properly formatted.
- **Use a meaningful subject line.** This is the first thing your reader will see, so use the space to help them understand the contents of the email even before they open it. So type in a subject that relates to the message you're sending.
- **Proof, spell-check, and use proper formatting.** Poor writing skills are a direct reflection on you!
- **Tone** - Remember the recipient cannot hear your tone of voice so choose your words carefully.

Guidelines and Reminders

- Email should be used for educational purposes only.
- Email transmissions may be monitored by staff at any time to ensure appropriate use. This means that teachers may check students' email.
- All email and all contents are property of the school.
- Email should only be used by the authorized owner of the account.
- Students need to protect their passwords.

Unacceptable Use Examples

- Non-educational related forwards (e.g. jokes, chain letters, images).
- Harassment, profanity, obscenity, racist terms.
- Cyber-bullying, hate mail discriminatory remarks.
- Email for individual profit or gain, advertisement, or political activities.
- Anything else deemed inappropriate by school personnel.

Copyright and Plagiarism

Students are expected to follow all copyright laws as outlined in [*Fair Use Doctrine of the United States Copyright Law* \(Title 17, USC\)](#). The distinction between what is fair use and what is infringement in a particular case will not always be clear or easily defined. There is no specific number of words, lines, or notes that may safely be taken without permission.

Acknowledging the source of the copyrighted material does not substitute for obtaining permission. Copyright protects the particular way authors have expressed themselves. The safest course is to get permission from the copyright owner before using copyrighted material.

Many people think of plagiarism as copying another's work or borrowing someone else's original ideas. To "Plagiarize" means that you are stealing and passing off the ideas or words of another as one's own. You should never use another person's work without crediting the source. In other words, plagiarism is an act of fraud. It involves both stealing someone else's work and lying about it afterward.

Technological advances such as ChatGPT are to be used as a learning aid (brainstorming and idea generation, research support, etc.), not a replacement for student work. Submitting work generated by AI as one's own original work is considered academic dishonesty.

Technology Discipline

Most tech-related behavior violations are equivalent to "traditional" classroom violations.

- Leaving your device at home is equivalent to leaving your textbook or school supplies at home.
- Cutting and pasting without citing sources or putting it into your own words is equivalent to plagiarism.
- Cyber-bullying is equivalent to bullying or harassment.
- Damaging or defacing the device or accessories is equivalent to vandalism or property damage.

In cases where unacceptable use or negligence is suspected, contact your school's administration.

Student access to computers is one way that SMCS enhances the learning opportunities for our students. Use of the devices is a privilege. Students who use a computing device at school are expected to follow SMCS's policies, procedures and practices specified in this handbook and the Responsible Use Procedures Agreement.

Accountability

Legal Title

Legal title to the device is with Saint Michael Catholic School and shall at all times remain with the school. The student is responsible at all times for the device's appropriate care and use. The device is specific to the student.

Legal Property

Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher or parent. Plagiarism is a violation of the student policy. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

Liability

The parent/guardian/student is responsible for the entire cost of repairs or replacement to computing devices damaged through student misuse, neglect, intentional damage or loss. In case of theft, an official police report will be required.

Digital Citizenship: Good To Know

What is Digital Citizenship?

- Digital Citizenship is a concept that helps students understand how to use technology appropriately in a society full of technology.
- The school expects students to use technology appropriately and responsibly whether in electronic communication or participation.
- The school has electronic precautions in place in order for students to participate safely and securely in this environment and enjoy the rights of a digital world in an educational setting.

School Responsibilities

- The school will provide Internet and email access to students.

- School staff will help students conduct research and ensure student compliance with the school's Responsible use Procedures.
- Filtering/blocking of inappropriate Internet materials is done at the school level, and the school provides network data storage areas for all students.
- Saint Michael Catholic School reserves the right to investigate the inappropriate use of resources and to review, monitor and restrict information stored on or transmitted via SMCS-owned equipment and resources.

Student Responsibilities

Students will abide by the school's Responsible use Procedures and:

- contact an administrator about any security issue they encounter.
- monitor all activity on their personal account(s).
- report email containing inappropriate or abusive language or questionable subject matter to a teacher or administrator at school.
- If a student is leaving SMCS, their device must be returned to the school prior to leaving.

Parent/Guardian Responsibilities

- Talk to your children about the values and standards you expect your children to follow as they use the Internet just as you talk to them about their use of all other media information sources such as television, telephone, movies, radio, etc.
- All school-issued devices contain Internet filters that are enabled at school and at home. Parents are encouraged to monitor student activity at home, especially their Internet use.

Appropriate Content

All files must be school appropriate. Inappropriate materials include explicit or implicit references to:

- Alcohol, tobacco or drugs
- Gangs
- Obscene language or nudity
- Bullying or harassment
- Discriminatory or prejudicial behavior

Monitor Student Use

The parent/guardian must agree to monitor student use at home, and away from school. The best way to keep students safe and on-task is to have a parent/guardian present and involved.

Suggestions

- Investigate parental controls available through your Internet/phone service provider and/or your wireless router.
- Develop a set of rules/expectations for device use at home. Some websites provide parent/child agreements for you to sign.
- Only allow device use in common rooms of the home (e.g. living room or kitchen) and not in bedrooms.
- Demonstrate a genuine interest in what your student is doing on the device. Ask questions and request that they show you his or her work often.
- Setting time limits for screen use is beneficial to give the eyes a break.

Health Tips for Parents

The average child in the US now spends an average of 7 hours a day using computers, cell phones, televisions and other electronic devices.

As screen and electronics time increases, time spent on exercise and family activities typically decreases. An increase in screen time has been shown to be linked to an increase in obesity rates.

So here's what you can do to help keep your child safe and healthy as he or she ventures into this new world of electronic education.

1. Limit the amount of time that your child is using the computer outside of schoolwork. The AAP recommends limiting total screen time to 2 hours daily.
2. Be aware of what your child is using the computer for. Know what Internet sites he/she is visiting and what he/she is doing on those sites.
3. Keep the bedroom as a screen free area. No televisions, cell phones or computers need to be in a child's bedroom, especially at night.
4. Encourage your child to get plenty of exercise daily.
5. Above all, talk with your child. Discuss what he/she is doing with her new computer and discuss things that have absolutely nothing to do with computers. Just talk!

Additional Articles

Healthy Habits for TV, Video Games, and the Internet by <http://kidshealth.org>

Turn Off the TV or Computer and Get Active by <http://www.healthykids.nsw.gov.au>

Cyber-Safety Tips

Open communication with your child is vital. Your child needs to feel they can come to you if they encounter frightening communications or images.

- **Set age limits.** Keep young children away from any unaccompanied chatting.
- **Understand the technology.** Open an account yourself, and get your whole family connected. If your child views the program as a way of staying in touch with family, there might be less risk of misuse with friends.
- **Model good video chat behavior.** Show children how to be polite and respectful, and let them know that's the behavior you expect when they're video chatting with their friends.
- **Use privacy settings.** Just like other communication tools like Facebook and Yahoo Messenger, most video chat programs come with privacy settings.
- **No inappropriate activities.** You can use parental controls through your Internet provider to restrict what sites your children can visit.
- **Set time limits.** With any online activity, be sure to tell your children how long they will have to engage in these activities.

E-Mail, IM and Chat Rooms - Help children stay safe online

- Know who your child is communicating with online.
- Open a family e-mail account to share with younger children.
- Teach your child never to open e-mails from unknown senders and to use settings on IM programs to block messages from people they do not know.
- Be aware of other ways your child may be going online—with cell phones, devices, or from friends' homes or the library.
- Tell your child not to share passwords with anyone but you to help avoid identity theft and cyberbullying.
- Familiarize yourself with popular acronyms at sites like www.netlingo.com and www.noslang.com/.

Help protect children against inappropriate content

- Use the NetSmartz [Internet Safety Pledges](http://www.net-smartz.org) to set clear guidelines for going online.
- Report the sexual exploitation or online enticement of a child to www.cybertipline.com.

Teach Your Children The Following Rules

- Never accept files or downloads from unknown sources; this includes familiar sources if you were not expecting them. Accepting files or downloads from unknown sources can bring a virus that could harm the

device.

- Never give out your real name, telephone or cell phone number(s), mailing address, or passwords. Giving away personal information can lead to identity theft or worse.
- Do not post photographs in publicly accessible sites. The settings for ANY social networking profiles should be PRIVATE and new friends are accepted only if they are known to the child AND parent.
- Posting pictures online or sending images can have dangerous consequences.
- Report Cyberbullying to an adult. (cyberbullying refers to the practice of using technology to harass, or bully, someone else).

Children's Internet Protection Act (CIPA)

The [Children's Internet Protection Act \(CIPA\)](#) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program.

Saint Michael Catholic School follows the Protecting Children in the 21st Century Act by:

- Blocking or filtering Internet access to materials that are harmful to minors
- Providing instruction in Internet Safety
- Monitoring online activities of minors

Children's Online Privacy Protection Act (COPPA)

The [Children's Online Privacy Protection Act](#) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

For our students to utilize modern, enriching educational tools, certain web-based programs and applications require the creation of student accounts. Under COPPA guidelines, schools are permitted to act as an agent for parents and provide consent for the collection of a student's limited personal data (typically a name, school-assigned email, or username).

Saint Michael Catholic School provides this consent *only* under the following strict conditions:

- **Educational Purpose Only:** The software or platform must be used solely for the benefit of the school's curriculum and the student's academic growth.
- **No Commercial Exploitation:** We ensure that approved vendors do not use student data for commercial profiling, behavioral marketing, or targeted advertising.

Vetting and Data Security

Our administration and technology team rigorously evaluate the privacy policies and terms of service of all digital platforms used in our classrooms—from our PK3 foundational programs through our 8th-grade academic tools. We only utilize platforms that maintain high standards of data security, encryption, and strict data-minimization practices. A complete registry of our primary school-wide approved digital platforms (such as **Google Workspace for Education, Clever, McGraw Hill, SuperKids, etc.**) is available upon request.

Contact your teacher if you have questions about any of the following....

- Troubleshooting
 - Always try restarting the device as the first step of troubleshooting.
 - **At School** - If restarting the device does not solve the problem, contact your teacher.

- **At Home** - If restarting the device does not solve the problem and it is an Internet connectivity problem, contact your Internet service provider. For other problems, contact your teacher when you return to school.
- How the device is used in instruction
- Question about the device
- Cyberbullying
- Inappropriate content
- Proper use of the device

Thank you for partnering with Saint Michael Catholic School by agreeing to abide by the Responsible Use Procedures (RUP) and becoming familiar with this *Technology Handbook for Parents and Students*.

