



St. Michael the Archangel High School

Acceptable Use Policy

2022-2023

The St. Michael the Archangel High School Acceptable Use Policy (AUP) applies to all technology resources. Students are expected to use all technology resources in a considerate, ethical, moral, legal, and responsible manner.

All St. Michael High School, school-issued Dell laptops/tablets and information stored on them are property of the school and are subject to the policies set forth by school administration and are subject to supervision and inspection. St. Michael High School reserves the right to monitor, access, retrieve, read, and disclose all messages, information, and files created, sent, posted from, and/or stored on the school issued device. School issued devices are subject to random checks by technology administrators for inappropriate installation and usage of software. Any student who violates this policy or any applicable local, state, or federal laws is subject to disciplinary action, a loss of technology privileges, and may face legal prosecution **at the discretion of local law enforcement.**

As technologies continue to evolve, so will this document. Each academic year, all students and parents of St. Michael High School must read and agree to abide by these standards. The administration of St. Michael High School reserves the right to amend any item in the Acceptable Use Policy or any technology policy during the year. Students will be notified of changes by email, and parents will be notified through the Principal's Newsletter.

Scope of Use

The digital world allows anytime, anywhere access. School hardware, software, and technology services are provided for academic excellence, faith development, and leadership skills. All students using said technology shall be accountable for its use. Technology should be used to support, enhance, and optimize the learning process. Students are expected to use all technology resources in a considerate, ethical, moral, and legal manner, ensuring their actions are consistent with the school's student handbook, which guides student behavior both on and off campus. Any threat to the school, or the individuals contained within it, shall be viewed as a violation of this AUP and those individuals may be subject to the disciplinary measures.

The types of electronic and digital communications referenced in this AUP include, but are not limited to, social networking sites or applications ("apps"), collaborative tools, cell phones, digital cameras, text messaging, email, Voice over IP, chat rooms, and instant messaging.

Privacy

All electronic resources owned or issued by St. Michael High School remain the property of the school unless otherwise agreed to in writing. The individual has no reasonable expectation of privacy. The school retains the right to monitor all electronic devices.

Each school-owned/issued technology device, account, and the information stored on them are property of the school and are subject to the policies set forth by school administration and are subject to supervision and inspection. The Diocese and St. Michael High School reserves the right to monitor, access, retrieve, read, and disclose any and all messages, information, and files created, sent, posted from, and/or stored on any school-owned/issued device or account.

General Computer and Internet Use

St. Michael the Archangel High School provides Internet access and network resources to students and employees who use the access in accordance with the mission of the school. Students must remember that technology devices and resources they are allowed to use are a privilege, not a right. By using such devices and resources, students agree to the following terms:

- Students are not allowed to install third-party applications on the computer that may interfere with the education process. (i.e.: games and Virtual Private Networks (VPN))
- Students are not allowed to stream or download games via the web or through a VPN or 3rd party application (i.e.: BlueStacks)
- Student use of the school's network and Internet usage must be consistent with the mission of St. Michael High School and its educational goals. Misuse includes any Internet conduct on or off campus that negatively affects the reputation of St. Michael High School including messages sent, posted, liked, shared, retweeted, or received that suggest harassment, racism, sexism, and inappropriate language and/or symbols.
- Students will not use their network resources or Internet access to monitor, interfere with or disrupt network users, services, St. Michael High School data or data of another student, or equipment, either on or off campus.
- Students will not access or try to make unauthorized entry to any computer accessible via the network or on remote networks. If a student notices a security problem, the student must notify administration immediately.
- Students will not use network resources or Internet access to transmit threatening, obscene, or harassing materials, including chain-letters, solicitations, inappropriate photos and videos, or broadcast messages via our network or email system.
- The Internet contains certain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. St. Michael students will not use network resources or Internet access to knowingly visit sites that contain this material nor import, transmit and/or transfer any of this material to other computers.
- Students may not capture or transmit any images, videos, or audio of school employees. Photographing and/or recording (by audio and/or video) of a teacher, staff member, student, or any other individual without permission is prohibited.
- Use of the school's network and internet usage must be consistent with the mission of St. Michael High School and its educational goals. Misuse includes, but is not limited to, any of the following: (i) any internet conduct on or off school campus which reflects negatively on St. Michael High School, including but not limited to sending or posting photos, images, videos, messages, or other communications that contain or suggest harassment, racism, sexism or inappropriate language and/or symbols; and, (ii) sending, transmitting or

displaying any unchristian, immoral, offensive, violent, pornographic, obscene or sexually-suggestive or explicit photos, images, videos, messages, or other communication in any form. Any such misuse, as determined by the school is strictly prohibited.

- Any student who receives a message suggesting harassment, racism, sexism, or the contents of which include inappropriate language, images, and/or symbols must immediately report the incident to a teacher, counselor, or administrator.
- Students will not provide any of their passwords or share another student's password with any other student or non-student. Students may not use another individual's account or log onto the Internet or network as anyone else.
- Students are responsible for all digital data, activity, and products on their school- owned and issued devices and accounts.
- For safety reasons, students will not communicate their address, phone number or other personal information to any person or company on the Internet or through email.
- While at school, students are required to access the internet using the St Michael High School Wi-Fi and are prohibited from connecting to secondary Wi-Fi devices such as a cellphone and/or other external devices. Children's Internet Protection Act (CIPA) laws require schools to filter internet access to students and block inappropriate content from being accessed. This includes internet tethering and mobile hotspots that enable (3G or 4G) access on the school issued laptops.
- The intentional destruction, deletion, or disablement of St. Michael High School installed software on any computer is prohibited. Unauthorized copying/installation of software programs belonging to the school is prohibited. Also, attempts to exceed or modify the boundaries set for the network are prohibited.
- Deleting, examining, copying, or modifying files and/or data belonging to the school is prohibited.
- Students may not change the background image/screen saver on their device nor the Office 365 account image which appears in their email.

Email and Communication Use

St. Michael the Archangel High School students will be issued a password protected login for the network, school email, and other communication resources. Students will use Office 365 for their school email account.

- Students are required to check their school email at least once every 24 hours.
- All communications sent or received serve as a representation of St. Michael High School.
 - Communication exchanged via the Internet or email must not damage the school's reputation.
- Instant messaging, chat rooms, social networking, gaming, email, and other electronic communication between students for non-academic purposes are prohibited unless these activities are directly related to class activities and/or participation.
- Students may not change their given email username.
- All email communication between faculty, staff, coaches, and students must be exchanged in an appropriate manner through the school-hosted email account.

- Students are responsible for reporting and rejecting any inappropriate materials and information received through electronic communication. Including spam or phishing emails.
- Students are prohibited from attempting to access or using another student's email.
- St. Michael High School reserves the right to access student email accounts for routine maintenance and to retrieve school records. Access also includes, but is not limited to, carrying out internal investigations, sending files to law enforcement, and accessing internet history, disclosed messages, and social networking data.
- Instant messaging, chat rooms, social networking, gaming, and email communication between students for non-academic purposes are prohibited during class time unless these activities are directly related to class activities and/or participation.

Online Learning Responsibilities/Expectations

- Students are reminded that all classroom expectations set forth by teachers and the handbook rules always apply. Failure to meet these expectations can result in both academic and behavioral consequences.
- Students are required to participate in all online class sessions. All video conferencing will be done utilizing Microsoft Teams.
 - When participating in online meetings and discussions:
 - Students should make every effort to find a quiet location other than a bedroom. If a bedroom must be used, students should not sit in or on a bed and should be aware of their surroundings which could be seen by the class. Nothing inappropriate should be displayed in the background.
 - School uniform is required.
 - To receive credit in class meetings, students must participate in class meetings by showing their face to the teachers and the class. Turning the webcam to the ceiling, floor, wall, or blocking the webcam is not acceptable.
 - Students should always be respectful and courteous to their teachers and classmates during online discussions and meetings.
- For roll call, students must check in to each class using Moodle. Important information including the class plan for the week is posted by their teachers.
- Students are responsible for maintaining all communication with their teachers, counselors, and administrators. Students should check their email daily and reply when necessary, within 24 hours.

Student Laptop/Tablet Responsibilities

All Dell laptops/tablets are property of St. Michael High School, and special care should be given to all devices. Students are responsible for their device from the time it is issued to the time it is returned to the school.

- Students are required to keep their laptop/tablet in the school provided carrying case. Failure to do so could result in disciplinary consequences. If a student experiences a problem with their carrying case, they should report the problem immediately to the Help Desk located on the St. Michael campus.

- Care should be taken daily to ensure that the laptop/tablet is not put in a situation where there is an increased risk for theft or damage.
- Students must report computer problems or issues to the Help Desk before school, during their lunch or immediately after school.
- Students are responsible for charging their laptop/tablets overnight and have them ready for use at school the following day. Failure to do so may result in consequences. Students are required to always have their power cords.
- All information stored on the computer should be backed up daily. This is the student's responsibility. The Help Desk is not responsible for files or information lost during computer reimaging or repair.
- During lunch, students are to keep their laptops/tablets packed in the carrying case while any food or drinks is present.

Help Desk and Customer Support

The St. Michael Help Desk is located next to the Library and is open on school days 6:45 a.m.- 2:45 p.m.

- Every attempt to seek help should be made before or after school or during lunch.
- The Help Desk is not responsible for lost files or notebooks that have not been backed up properly.
- Students should only go to the Help Desk during class if the issue is preventing them from participating in a class activity or assignment. Students are prohibited from going to the Help Desk during class time without a signed permission slip from a teacher.
- Students should always RESTART their laptop/tablet before going to the Help Desk.
- Students should always BACKUP their laptop/tablet before going to the Help Desk.
- Students other than St. Michael Help Desk employees are prohibited from entering the Help Desk designated areas.

Damage/Malfunction

- Accidental damage insurance purchased by SMHS may cover the cost of the repair.
- If the computer malfunctions or is damaged, any repair costs not covered by the accidental damage insurance is solely the responsibility of the student and the parent.
- If the computer is lost or stolen, the replacement cost is solely the responsibility of the student and the parent.
- Damage and theft insurance is available through outside vendors. Purchasing this optional insurance in no way eliminates or limits the responsibility of the student and the parent to pay SMHS for repairs or replacement of the computer.

- In the case of theft of a school owned/issued device, parents are required to notify the school and file a police report within 24 hours of being discovered. Misplaced/lost devices should be reported to school personnel immediately. If the device is not recovered, the parent/guardian is responsible for the replacement cost of the device.
- Purposeful or careless damage to school-owned/issued devices is prohibited. The individual will be responsible for any repair or replacement costs. The school has the discretion to suspend each user's technology privileges and/or take disciplinary action.
- Students are required to keep all labels, barcodes, and stickers on their device. Removal of these items will result in a defacing charge of \$10.00 per incident.

Replacement Costs

- Stylus - \$70.00
- AAAA battery for stylus - \$1.00
- Barcode/sticker/label replacement - \$10.00 per incident
- Computer Charger - \$45.00
- Flak Jacket (carrying case) - \$35
- Dell Laptop - \$1365

Cellular Devices

St. Michael High School recognizes the convenience, logistical and safety advantages for students to have cellular telephones and other communication devices in their possession while on campus and during school activities.

- Communication devices must be turned off and stowed away throughout the academic day, including without limitation during school activities, and may not be displayed.
- Students may use communication devices while on school campus and during school activities only with the permission of the supervising adult, such as the teacher, bus driver, athletic coach, or sponsor.
- The use of cellular devices in an unacceptable manner in the school setting is prohibited. Examples of unacceptable usage include, but are not limited to, the following: use of a device for any purpose inside a restroom or locker room, use of a device on the school campus for cheating, cyber bullying, sexting, or taking inappropriate photos or videos.
- Violations of this AUP may result in disciplinary measures as well as the confiscation of the communication device.