

Technology Policy: Resources, Access, Safety, and System
Midlands Middle College

**As listed and approved in the Student Handbook*

MMC's network system has been established for a limited educational purpose, including but not limited to classroom-based projects and student works, college and career explorations, and high-quality, academically enriching research. Recognizing the value of the Internet, the school supports teachers and students being engaged in an online environment that allows them to discuss, collaborate, communicate, create, and share in a safe, ethical, and responsible manner. MMC will provide each student a device which is connected to the MMC network for use in each class. **Personal devices will not be allowed/utilized.**

The school has the right to place reasonable restrictions on the material students access or post through the system. Students are expected to follow the rules set forth in this handbook and the law in their use of the network system. Additionally, the MMC system will employ update firewall measures and filtering to ensure obscene, pornographic, or harmful content.

ACCESS TO ONLINE MATERIALS

- The material students access through the network system should be for class assignments or for other, legitimate educational objectives. Students are not to post non-academic messages to others within the network system.
- Use of the network system for entertainment purposes (e.g., accessing social networking sites, including but not limited to SnapChat, Facebook, and YouTube) is not allowed.
- If a student mistakenly accesses inappropriate information, the student should immediately report this access to a teacher or an administrator. This will protect the student against a claim of intentionally violating this policy.
- The school has taken reasonable steps to restrict access to materials it considers harmful and to materials that do not support or conform to accepted educational objectives.
 - Students will not use the network system to access the following: material that is obscene; child pornography; material that depicts, or describes in an offensive way, violence, nudity, sex, death, or bodily functions; material that has been designated as for adults only; material that promotes or advocates illegal activities; material that promotes the use of alcohol or tobacco, school cheating, or weapons; or material that advocates participation in hate groups or other potentially dangerous groups.
 - If a student feels that the filtering software is blocking access to an appropriate site, the student should report this to a teacher or administrator.
 - Students will not seek to bypass the network by using a proxy site or some other technology, such as USB flash drives or discs.
- The use of the network system is a revocable privilege for all users.

COMMUNICATION SAFETY EXPECTATIONS

- “Personal contact information” includes a student’s full name, together with other information that would allow an individual to locate him/her, including family name, home address or location, work address or location, or phone number.
- Students may disclose personal contact information to educational institutions, companies or other entities for college/career exploration purposes, or with specific staff approval.
- Students will not disclose names, personal contact information, or any other private or personal information about other students. Students will not forward a message that was sent privately without permission of the person who sent the message.
- Students will promptly disclose to a teacher or other school staff member any message received that is inappropriate or makes him/her feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

UNLAWFUL, UNETHICAL, UNAUTHORIZED, AND INAPPROPRIATE USES AND ACTIVITIES

- Unlawful Activities
 - Students will not attempt to gain unauthorized access to the network system. This includes attempting to log in through another person’s account or to access another person’s files.
 - Students will not make deliberate attempts to disrupt the network system or any other computer system or destroy data by spreading computer viruses or by any other means.
 - Students will not vandalize the computer equipment by disassembling or disconnecting any computer components or peripherals.
 - Students will not engage in any conduct that modifies, harms, or destroys any computer or network hardware, such as mice, keyboards, and components that reboot computers.
 - Students will not use the Internet system to engage in any other unlawful hacking activities such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or threatening the safety of any person (including public officials).
- Inappropriate Language and Unauthorized/Unethical Activities
 - Restrictions against inappropriate language apply to all speech communicated through the network system, including public messages, private messages, and material posted on Web pages.
 - Students will not use obscene, profane, lewd, sexually oriented, vulgar, rude, inflammatory, threatening, or disrespectful language.

- Students will not use, access, transmit, or download information that is hate-motivated, fraudulent, abusive, or racially offensive.
- Students will not knowingly or recklessly post false or defamatory information that could cause damage or a disruption to your school or any other organization or person.
- Students will not use a camera phone to record or take pictures of students or staff anywhere on campus and post on the Internet (e.g., YouTube) without the school's permission.
- Students will not engage in personal attacks, including prejudicial or discriminatory attacks, or harass or bully another person.
- Students will not use, access, transmit, or download information that relates to or encourages the illegal use of controlled substances or other criminal conduct. ○ Students will promptly disclose to a teacher or another school employee any message received from any other student that is in violation of the restrictions on inappropriate language and unauthorized activities.
- Plagiarism and Copyright Infringement
 - Students will not plagiarize works found on the Internet. Plagiarism is taking the ideas, graphics, or writings of others and presenting them as if they were yours without adequate and accurate citation.
 - Students will respect the rights of copyright owners in use of materials found on, disseminated through, or posted to the Internet. Copyright infringement occurs when a student reproduces a work that is protected by a copyright without explicit permission from the copyright holder or outside the limitations of copyright law.
 - Students will not use peer-to-peer file sharing programs, such as “BitTorrent” or “Limewire,” to download or share copyrighted movies, music, or games.
 - Students will not share their individual work with another student to be used for meeting assignment requirements.
 - Students will not utilize AI sites such as ChatGPT to create documents or complete assignments.

SYSTEM SECURITY

- Students are responsible for their own individual accounts and should take all reasonable precautions to prevent others from being able to access them. Under no conditions should a student provide his/her password to another person. Students should protect their files and accounts by logging out and regularly backing up personal files.
- Students will immediately notify a teacher or an administrator if they identify a possible security problem. However, students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

- Students will not engage in any conduct or activities that could disrupt the use of the system for others, including installing programs or files, deleting programs or files, modifying settings, changing passwords, or reconfiguring the system.

MMC AND MTC RESOURCES

- Each classroom contains technology resources that have been purchased by MMC and are available for student use while at MMC. Students will not remove these resources from any classroom, not even to move to another classroom, without express permission from a teacher or other staff member.
- Students will not under any circumstances remove technology resources from the school campus. School devices may not be taken home for personal use.
- MMC provides a school-issued Google account to all students. This is part of a set of tools called “G Suite for Education” being used in classrooms, which opens the opportunity for students to practice the appropriate use of professional email and gives them a tool with immediate use in their academic life, including communicating with teachers, other students, colleges, and more. With this educational opportunity also comes responsibility. It is important that parents and students read Google’s privacy information available at <https://www.google.com/edu/trust/> and together discuss the rules for appropriate email use. Student email may be monitored for inappropriate use, which could result in the loss of this privilege as well as possible disciplinary action.

HOME USE OF MMC CHROMEBOOKS

On rare occasions, a student may need to utilize an MMC Chromebook at home to complete school assignments. Students may only ask to utilize the Chromebook if they do not have access to other appropriate technology to complete schoolwork. In these instances, students must check the device out overnight through the front office on a first come first serve basis as devices are limited. MMC will maintain a list of students identified by their parent/guardian as not having a reliable device at home and will utilize this list in determining check-out privileges. The device must be returned to school the following day. Students assume responsibility for the care and appropriate use of the device while in their possession. Students utilizing school devices at home are required to follow all school policies for use of technology outlined above.