2023-24 TECHNOLOGY AND COMPUTER USE POLICY

Mercy High School requires students to possess a school approved technology device that will be the student's responsibility to obtain. Students must bring their device AND charging cord to all classes. Mercy High School is not responsible for theft or damage to any student's device. Any student damaging another student or faculty device is financially responsible for repair/replacement of the damaged device. Keeping the serial number of the device is a good practice in the event of loss or damage. The device is intended to support the educational objectives of Mercy High School. The use of the device is a privilege, not a right. Proper usage is based on trust and good judgment by all parties involved. Failure to adhere to these standards will result in disciplinary action and legal action if applicable. The following terms and conditions are meant to provide families with examples of prohibited conduct but are not intended to serve as an exclusive list. Students may be disciplined for engaging in other conduct deemed by the sole discretion of the school or teaching staff as detrimental to the school and its mission, and/or harmful to other students, faculty or the school community.

Lab Behavior All Mercy High School standards of conduct apply in the computer production labs and library/media center. Labs are intended for educational purposes. No food or drink is to be brought to the labs or placed near any classroom computer at any time. All printing should be for educational purposes and printing must be completed in the library/media center. Methods to decrease the amount of paper being used are encouraged. These include printing in smaller fonts or copying article text to a Word document to avoid pictures and or advertisements being printed.

Proper Usage All technology resources are intended to promote educational excellence. All school approved electronic devices are to be used only for academic and school-related purposes. If inappropriate information or websites are accidentally accessed the student should inform a staff member immediately. CELL PHONES ARE NOT SCHOOL APPROVED DEVICES. Students are able to communicate with parents or family members about incidental logistical and scheduling matters during appropriate times and with school approval. The following are examples of activities **NOT** permitted:

- Contacting parent/guardian via text or email to relay notification of student illness or student desire to leave school
- Taking photos or video of anyone on campus without that person's direct permission
- Engaging in instant messages for purposes that are not academic and school-related
- Accessing or using any web log (blog), forum, "social network" web site, or app of any kind, including but not limited to Facebook, Twitter, Tumblr, Snapchat, Instagram, etc.
- Posting information and/or messages on any social networking site such as Facebook and Twitter
- Accessing or using chat rooms for purposes that are not academic or school-related
- Sending obscene messages or using obscene language
- Harassing another person or participating in cyberbullying
- Knowingly or recklessly posting false or defamatory information about any person or organization
- Engaging in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.
- Posting chain letters or engage in "spamming" (spamming is defined as the use of electronic messaging to send unsolicited bulk messages.)
- Participating in online contests, advertising, political lobbying, gambling, or shopping
- Accessing, sending, or retrieving pornographic material
- Falsifying one's identity to others (also known as catfishing)

- Posting, sending, or downloading copyrighted material without permission. Users are to respect the rights and intellectual property of others in accordance with state and federal copyright laws. Transferring copyrighted material to or from the school's computer without the expressed permission of the owner can be a violation of federal law
- Engaging in the unauthorized exploration of Mercy's network or other computer infrastructure
- Circumventing security measures on school or remote computers or networks (hacking)
- Attempting to gain unauthorized access to another's resources, programs, or data
- Posting text files or other files dangerous to the integrity of any network
- Disclosing the personal information of others that may be stored on the school system such as age, address, and phone number
- Any other activity deemed inappropriate by Mercy Staff and Administration

Communication is Not Private Each student's online communication is a reflection of our school. E-mail, instant messages and other forms of electronic communication to and from our school's network is like a postcard: it is not private and may be monitored as needed. Therefore, students have no right to privacy as it relates to use of the school's electronic resources. The school has the right to monitor all communications through or on its servers, electronic equipment and school provided internet. Additionally, teachers may examine electronic equipment that belongs to the student in any situation where they might reasonably question the student's academic integrity or honesty or suspect that it has been used in a violation of the law or of school policies or rules.

Security It is essential that school computers never be disrupted by any virus. For that reason, only attempt to access information that is deemed safe from trusted sources. Students agree to report any misuse of the system to an appropriate staff member. Students agree to respect others' privacy and not use another person's account or password, even with that person's consent. Students must also not disclose or allow others to use their passwords. Devices not being carried by the student must be locked in a safe place to reduce the risk of theft or damage.

Wireless Access Students accessing the internet on campus must do so through the school's wireless connection. Any use of personal hotspots or other alternative means of internet access is strictly prohibited. Students are only allowed to have one device connected to the wireless network and are encouraged to turn off Wi-Fi signal when devices are not in use. When the entire school community is gathering in one area of the building, Wi-Fi must be turned off to eliminate the stress on the wireless network. Students are also forbidden to use VPNs while connected to school access points. Failure to comply may result in disciplinary action and student wi-fi privileges being revoked.

Copyright & Plagiarism Students are responsible for producing their own work in completing school assignments. Downloading and copying another individual's work from the internet without crediting the author is plagiarism. Copyright violations can include the copying of computer software or written materials without the permission of the author.

Email Usage and Etiquette Any email correspondence regarding school or school projects should be conducted only using the student's school issued account. Teachers and staff will not respond to a student who is using her personal email. This policy is in place to increase our cybersecurity. Students should understand that email is a medium of communication and appropriate language and etiquette must be used when sending email. This conduct includes communication with teachers, staff and other students. Email should contain correct punctuation and grammar. It should also be understood that email is not confidential by nature. Students must promptly disclose to a teacher or administrator any inappropriate or questionable email communication.

Virtual Meetings Virtual meetings (ex. Google Meet, Zoom, etc.) are used by Mercy Faculty for remote individual and small group work sessions with students. The times and dates for the virtual meetings are posted for all students enrolled in a teacher's class. The recorded virtual meetings are open sessions and the teacher may be working with one or more students during the designated time frame. An administrator has the option to join all virtual sessions.