MERRILL COMMUNITY SCHOOLS

NETWORK/INTERNET ACCEPTABLE USE POLICY

AND BYOD (Bring Your Own Device) POLICY

Use of the Merrill Community School District’s educational technology, including student access and use of the Internet through the MCS/Net (Merrill Community School Network) is **strictly limited to legitimate educational purposes**. It is to be used solely to support and enhance the School District’s curriculum in a manner, which is consistent with the Merrill Community School District’s mission statement.

Access to the MCS/Net includes an individual directory as well as Internet privileges. The network administrator reserves the right to monitor ALL activity on the system. Network storage areas are subject to inspection without notice at the request of any staff member. This is necessary to maintain system integrity and to insure that users are using the system responsibly. Users should not expect that files stored on district servers will be private. This storage space, like the whole system, should be used exclusively to store files that are directly related to course work.

In compliance with the Children’s Internet Protection Act (CIPA) Merrill Community Schools will filter Internet access and protect children from child pornography, obscene materials and materials harmful to minors and adults. Merrill Community Schools will implement an Internet safety policy addressed in the body of this Acceptable Use Policy.

Use of the MCS/Net and stand-alone computers is governed by the following rules:

1. Students may use the network only after the school has received the “Network Access Agreement”, signed by the student and parent.
2. Students are solely responsible for their own user-ID and passwords. Sharing passwords or using another’s password is prohibited. Students are accountable for any misuse of the systems done under their login. If you suspect your password has been compromised, see the network administrator immediately to change it.
3. As stated earlier, the MCS/Net and Internet access are intended for educational purposes only. This prohibits actions such as: using chat rooms, using personal e-mail, playing non-educational games, etc. and downloading and/or storing any data in your network drive which is not directly related to coursework.
4. All students will be educated about appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.
5. Vandalism to a computer system can take many forms, and is prohibited by this policy. Vandalism might include, but is not limited to:
* installing or removing software from a computer or network drive
* downloading or storing any data on the computer
* storing data on the network other than in your assigned network drive
* damaging the computer and its peripherals (monitor, keyboard, mouse, scanner, mouse pad, etc) in any way
* removing any items from the computer or its peripherals
* rendering the computer or the network inoperable
* performing any act that diminishes the performance of the computer or the network
* gaining unauthorized entry into a file for any purpose
* introducing a virus, either intentionally or through irresponsible handling of data and telecommunications resources

The network administrator may define additional areas of vandalism.

1. The purchase, sale, and/or advertisement of goods or services via the Internet is prohibited
2. Violation of copyright, trademark, trade secrets, or licensing agreements is prohibited
3. Users of the MCS/Net must not use the system to access information or communications that are indecent, profane, vulgar, threatening, defamatory, or an invasion of privacy. A user who unknowingly does this should inform a staff member immediately. The network must not be used for anything other than teacher supervised, course related work.
4. Users of the MCS/Net are responsible for respecting and adhering to local, state, federal, and international laws.
5. Student Internet activities will be monitored by the District to ensure that students are not accessing inappropriate sites. Each District computer with Internet access has a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors.
6. The MSC/Net is a monitored network and no stated or implied guarantee is made regarding the privacy of any communications, or storage space.
7. The District does not guarantee that the functions of the system will meet any specific requirements the user may have, or that it will be error free or uninterrupted.
8. The District shall not be liable for any direct or indirect, incidental or consequential damages (including, but not limited to, lost data, information, time, or any harm caused by exposure to offensive material) sustained or incurred in connection with the use and operation of the system or the inability to use the system.
9. The user may be required to make full financial restitution for unauthorized expenses incurred through the use of educational technology inconsistent with the agreement.
10. The use of the MCS/Net is a privilege, not a right, and inappropriate use will result in disciplinary action. In the event a violation of this agreement occurs, the following procedure is followed:
* the staff member observing the violation fills out the AUP violation form
* the form is turned in to the building administrator
* a review committee meets to review the violation
* the user and parent are notified of the committee’s decision
* if the user feels the punishment is unfair or unwarranted, he/she is given an opportunity to address the committee
1. A user’s access to the MCS/Net will be terminated immediately after the user leaves the Merrill Community School District.

### Policies Regarding Personal Devices

Students may bring personal computing devices to school with parental permission and as long as they understand the following requirements:

1. Students may not connect to any network (cellular or WiFi) outside of the school district’s wireless network.
2. The student understands that they have no privacy regarding their personal device and that school personnel may inspect the device for videos, texts, emails, Internet history or other content. The student agrees to unlock their device for inspection.
3. The student may only use the device before school, after school at lunch (High School and Middle School only) or at other times specifically approved of by a teacher.
4. There will be not personal cell phone use allowed during the school day.
5. The student agrees to turn the device off when instructed by a school employee for any reason.
6. The student must have updated anti-virus, anti-malware and other security software installed when possible.
7. The student brings the device to school at their own risk. Damage or theft of the device is not the responsibility of the school.
8. The school may install or ask the student to install software that monitors the device’s use.
9. The device may not be used for:
	1. Sexting
	2. Academic dishonesty
	3. Disruption of the teaching/learning environment
	4. Violations of other person’s privacy
	5. Actions compromising personal or school safety
	6. Any unethical or illegal activity
	7. Cyberbullying
10. The student may not:
	1. Download software, open email or run macros from an unknown source.
	2. Run network-related tools or diagnostics as a user of the district’s computer network.
	3. Degrade the performance of the data network.
	4. Access, upload, download or distribute inappropriate material.
	5. Violate copyright or use others’ intellectual property without permission.
	6. Reveal any personal information.
	7. Transmit, receive or download any materials promoting the use of drugs, tobacco or alcohol.
	8. Instant message others.
	9. Sell or purchase any illegal substance.
11. The district reserves the right to prevent the student from using the device for any reason and at any time.

### Disciplinary Procedures:

The following consequences apply to the school’s AUP as it regards to school owned devices and personal devices.

The administration reserves the right to adjust the following disciplinary procedures in special circumstances.

Following are the typical and recommended penalties for AUP violations:

1st offense: 5 day suspension of computer use and or denial of Internet access

2nd offense: 10 day suspension of computer use and or denial of Internet access

3rd offense: 90 day suspension of computer use and or denial of Internet access

4th offense: account disabled for rest of school year and or denial of Internet access

If a major violation is committed, the administration reserves the right to go directly to suspension and revoke any and all computer privileges.