6200.

STUDENT ACCEPTABLE USE POLICY 6200

Computers, computer networks, electronic devices, Internet access, and email are effective and important technological resources. The Board of Education may provide computers, a computer network, including Internet access, and an email system, as well as other electronic devices that access the network(s), referred collectively as the "computer systems." The Board of Education and the Administration believe in the educational value of such computer systems as technological resources and recognize their potential to support our curriculum by expanding resources available for staff and student use. The Meriden Board of Education provides these computer systems in order to enhance the educational opportunities for students and the business operations of the school district.

Terms of Use

1. **Acceptable Use:** Student access to the District's computer systems must be solely for education-related purposes. Use of the computer systems will be allowed only for students who act in a considerate and responsible manner in using such systems.
2. **Privileges:** The District's technological resources are expensive to purchase, install, and maintain. As such, ***use of these technological resources is a privilege, not a right***, and violations of standards of conduct required by this policy may result in a revocation of access privileges and/or discipline in accordance with the Board's student discipline policy. Students will be required to adhere to certain policies and procedures, as outlined below. The appropriate building principal may make all decisions regarding whether or not a user has authorization to use any and all of these resources and may deny, revoke, or suspend access at any time; his or her decision is final.
3. **Monitoring**: Students are responsible for good behavior on school computer systems just as they are in other school settings. General school rules for behavior and communications apply. It is expected that users will comply with district standards and will act in a responsible and legal manner, at all times in accordance with district standards, state, and federal laws.

It is important that students and parents/guardians understand that ***the district, as the owner of the computer systems, reserves the right to monitor and review the use of these computer systems.*** The district intends to monitor and review in a limited fashion, but will do so as needed to ensure that the systems are being used for district-related educational purposes.

As part of the monitoring and reviewing process, the district will retain the capacity to bypass any individual password of a student or other user. The system's security aspects, such as personal passwords and the message delete function for email can be bypassed for these purposes. ***All users must be aware that they should not have any expectation of personal privacy in the use of these computer systems.***

1. **Unacceptable Use:** Students are permitted to use the district's computer systems for legitimate educational purposes. The user is responsible for his or her actions and activities

involving the network. Conduct which constitutes inappropriate use includes, but is not limited to, the following:

2. Using the computer networks for any activity that is generally prohibited by law, by Board policy, or school rules or regulations. Use of these computer systems for the purpose of carrying out such behavior or activity is prohibited.
3. Sending any form of harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime).
4. Gaining or seeking to gain unauthorized access to computer systems.
5. Damaging computers, computer files, computer systems, or computer networks.
6. Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from a teacher or administrator.
7. **Using another person's password under any circumstances.**
8. Trespassing in or tampering with any other person's folders, work, or files.
9. Sending any message that breaches the district's confidentiality requirements, or the confidentiality of students.
10. Sending any copyrighted material over the system.
11. Using computer systems for any personal purpose, or in a manner that interferes with the district's educational programs.
12. Accessing or attempting to access any material that is obscene, contains child pornography, or is harmful to minors.
13. Transmitting or receiving email communications or accessing information on the Internet for non-educational purposes.
14.
15. Accessing or attempting to access social networking sites (i.e., Facebook, Twitter, Myspace, etc.) without a legitimate educational purpose.

Misuse of the computer systems, or violations of this policy, may result in loss of access to such computer systems as well as other disciplinary action up to and including suspension and/or expulsion, depending on the specific conduct.

Anyone who is aware of problems with, or misuse of, the computer systems, or has a question regarding the proper use thereof, should report this to his or her teacher or principal immediately. The Board and Administration urge any student who receives any harassing, threatening, intimidating, or other improper message through the computer systems to report it immediately. It is the Board's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message. ***Please report such events***.

1. Internet Safety:

The Administration will take measures to: assure the safety and security of students when using forms of direct electronic communications; prohibit unauthorized access, including "hacking" and other unlawful activities by minors online; to prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; to education minor

students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bulling awareness and response; and to restrict students' access to online materials harmful to minors, including obscene materials and child pornography.

The district will provide supervision for students while they are using district computer systems in order to promote students' compliance with the foregoing terms and conditions for use. Decisions regarding supervision of use will be made in the judgment of the administration, based upon factors such as, but not limited to, the age of the students using the district's computer systems, and the circumstances of such use.

The Board will implement a technology protection measure to block or filter Internet access to visual depictions that contain obscene material, contain child pornography, or are harmful to minors, and ensure that such filtering technology is operative during computer use by minor students.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250 et seq. (computer-related offenses)

Conn. Gen. Stat. § 53a-194 (definition of obscene)

Children's Internet Protection Act, Pub. L. 106-554, codified at 47 U.S.C. § 254(h)

Electronic Communication Privacy Act of 1986, Pub. L. 99-508, codified at 18 U.S.C. §§ 2510-2520

Protecting Children in the 21st Century Act, Pub. L. 110-385, codified at 47 U.S.C. § 254(h)(5)(B)(iii)

Every Student Succeeds Act, Pub. L. 114-95, codified at 20 U.S.C. § 6301 *et seq*.

18 U.S.C. § 2256 (definition of child pornography)

Miller v. California, 413 U.S. 15 (1973) (definition of obscene)

Approved October 9, 2001

Amended March 23, 2004

Amended November 21, 2017

Previous Policy Number HH1.3R and 6141.3211-R

6200.1(E).

Click link to view the Student Acceptable User Policy Cover letter: AUP Student Cover Letter

6200.2 (E).

Click on the link to view the Student Acceptable Use Agreement.

/uploads/6200_2-E_AUP_Agreement_Form.pdf