MONITEAU SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMPUTER TECHNOLOGY

ADOPTED: October 25, 2010

REVISED: June 25, 2012, October 13, 2014 July 8, 2015

815. ACCEPTABLE USE OF COMPUTER TECHNOLOGY

1. Purpose

The Board supports use of the Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

2. Definitions

Telecommunications is a system that allows users access to a wide variety of information from electronic networks found on local, state, national and international data bases. Examples include Internet, e-mail, discussion groups and bulletin boards. These accounts are intended for the sole use of educators and other authorized users.

Harmful to minors shall mean any picture, image, graphic image, file, or other visual or written depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion.

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals.

3. Lacks serious literary, artistic, political, or scientific value as to minors.

3. Authority

The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

	The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. The district reserves the right to log network use and to monitor fileserver space utilization by district users, including, but not limited to, e-mail messages and accounts, user files located on local or network drives, and Internet content access while respecting the privacy rights of both district users and outside users. The Board establishes that use of the district network and other computing resources is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action. District network administrators have the right to deny, revoke, or suspend specific use. Students may only access the Internet after reading the Acceptable Use Policy of Computer Technology in their Student/Parent Handbook.
47 U.S.C. Sec. 254	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his/her use of the computer network and Internet and stay away from these sites. If a student finds that other users are visiting offensive or harmful sites, s/he should report such use to his/her supervising teacher.
4. Delegation of Responsibility	The district shall make every effort to ensure that this resource is used responsibly by students, staff and community members. The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The building administrator and/or the Director of Technology shall have the authority to determine what is inappropriate use; his/her decision shall be final.

20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
5. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system. Individual computing classrooms or areas may impose printing restrictions on any or all users in that area. <u>Prohibitions</u> Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Any violation of the use of the district computing resources should be reported to the teacher, the principal, and the Director of Technology. Specifically, the following uses are prohibited: 1. Facilitating illegal activity. 2. Commercial or for-profit purposes. 3. Nonwork or nonschool-related work, including personal entertainment or private activities. 4. Product advertisement or political lobbying. 5. Hate mail, harassment, discriminatory remarks, and offensive or inflammatory communication.

6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

7. Access to or printing of obscene or pornographic material or child pornography, inappropriate text files, or files dangerous to the integrity of the local area network is prohibited.

8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

9. Inappropriate language or profanity.

10. Transmission of material likely to be offensive or objectionable to recipients.

11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

12. Impersonation of another user, anonymity, and pseudonyms.

13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.

14. Loading or using of unauthorized games, applications, programs, files, or other electronic media without the expressed written consent of the Director of Technology.

15. Disruption of the work of other users.

16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

17. Quoting of personal communications in a public forum without the original author's prior consent.

18. Malicious use of the network to harass other users or infiltrate a computer or computing system is prohibited.

19. Altering a network or computing resource, device, peripheral, file, or folder names.

20. Copying application, folders, or files unless it is directly related to curriculum projects and it follows all other established policies and guidelines.

21. Distributing or altering network or computing resource passwords.

22. Users may not use any network or computing resource to gain unauthorized access to other networks or computing resources.

23. Users may not violate any software or other licensing agreements.

24. Installing, previewing, or copying software to the network or any computer.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet, other networks, or district software and hardware; this includes but is not limited to uploading or creating computer viruses.

Pol. 218, 317	The violations contained within this policy are not all inclusive, only representative and illustrative. A user who commits an act of misconduct which is not listed may also be subject to disciplinary action. After administrative investigation, disciplinary consequences will be determined by th levels of progressive discipline. Administrators may use any or all of the following suggested intervention strategies and disciplinary action. *Minimum Actions* – 1. Administrator/Teacher/Student conference. 2. Administrator/Teacher/Student verbal and/or written reprimand. *Additional Actions As Deemed Appropriate* – 1. Administrator/Parental contact. 2. Referrals and conferences involving various support staff or agencies. 3. Behavioral contracts. 4. Required serving a minimum of one (1) day suspension from using all district computer equipment. 5. Confiscation of inappropriate items. 6. Restitution/Restoration, including any professional services required. 7. Denial of participation in class activities. 8. Banned from access to the Internet for a specified number of days. 9. Banned from using all computer equipment, networks, or Internet.
Pol. 233	10. In-school suspension.
Pol. 233	11. Out-of-school suspension.
Pol. 233	12. Expulsion.

	13. Other intervention strategies as needed. 14. Subject to criminal prosecution under state and federal laws. <u>Copyright</u> The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information such as home address or telephone number to other users on the network, including chat rooms, e-mail, Internet, etc. Users shall not use their real last name or any other information which might allow a person to locate the user without first obtaining the permission of a supervising teacher. Users shall not arrange a face-to-face meeting with someone they met on the computer network or Internet. If someone attempts to arrange a meeting with a user as a result of an Internet contact, the user shall report the communication immediately to a supervising teacher.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minors' access to materials harmful to them.

Confidentiality Of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent/guardian. Users should never give out private or confidential information about themselves or others in the Internet, particularly credit card numbers and Social Security numbers. Only a member of the school administration may authorize the release of student information.

Active Restriction Measures

The district, either by itself or in combination with an Internet Service Provider (ISP), will utilize filtering software or other technologies to prevent students from accessing visual depictions that are obscene, child pornography, or harmful to minors. The district will also monitor the online activities of users, through direct observation and/or technological means, to ensure that users are not accessing such depictions or any other material that is inappropriate for minors. Internet filtering software or other technology-based protection systems may be disabled by the Technology Coordinator or his/her designee, as necessary, for purposes of valid research or other educational projects being conducted by a user.

Warranties/Indemnification

The district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The district shall not be responsible for any claims, losses, damages or costs, including fees, of any kind suffered, directly or indirectly, by any user or his/her parent/guardian arising out of the use of its computer networks or the Internet under this policy. By signing this policy, the user is taking full responsibility for his/her use, and the user who is eighteen (18) or older or, in the case of a user under eighteen (18), the parent/guardian agree to indemnify and hold the district, administrators, professional employees, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent/guardian agree to cooperate with the district in the event of the district's initiating an investigation of a user's access to the computer network and the Internet.

	Updates Users, or the user's parents/guardians, may be asked to provide new or additional registration and account information or to sign a new policy. The policy must be signed if the user wishes to continue to receive service. If after users have provided account information, some or all of the information changes, users must notify the building principal. References: School Code – 24 P.S. Sec. 1303.1-A Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777 Internet Safety – 47 U.S.C. Sec. 254 Board Policy – 249, 814

Moniteau School District
Network and Internet Access

STUDENT CONSENT AND WAIVER

The following form must be read by the student and signed by the student and his/her parent or legal guardian.

By signing this Consent and Waiver Form, I agree to abide by the following restrictions. I have discussed these rights and responsibilities with my parent(s)/guardian(s).

Further, my parent(s)/guardian(s) and I have been advised that the district does not have control of the information on the Internet, although it attempts to provide prudent and available barriers. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people. While the district's intent is to make Internet access available to further its educational goals and objectives, account holders may have the ability to access other materials as well.

The district believes that the benefits to educators and students from access to the Internet, in the form of information resources and opportunities for collaboration, far exceed any disadvantages of access. Ultimately, the parent(s)/guardian(s) of minors are responsible for setting and conveying the standards that their student should follow. To that end, the district supports and respects each family's right to decide whether or not to apply for Moniteau district network access.

Any questions should be directed to the Director of Technology at (724) 637-2117 ext. 124 or the building principal.

The student and his/her parent(s)/guardian(s) must understand that student access to the district network exists to support the district's educational responsibilities and mission. The specific conditions and services that are offered will change from time to time. In addition, the district makes no warranties with respect to the district network service, and it specifically assumes no responsibilities for:

1. The content of any advice or information received by a student from a source outside the district, or any costs or charges incurred as a result of seeing or accepting such advice.

2. Any costs, liability or damages caused by the way the student chooses to use his/her district network access.

3. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the district.

4. Electronic mail (email) will be provided to every student/staff in the District. These accounts are District owned accounts and are for educational purposes only. The email account issued to the student/staff will be the only email account allowed to be accessed on the District's network.

5. With a multitude of wireless devices available, the District will not guarantee that all devices will work on the BYOD network and will take no responsibility for devices that are not compatible.

6. All devices must be registered with the Technology Department prior to accessing the network. Students/staff may have up to three devices registered at any given time.

7. The district or its employees shall not be liable for the loss, damage, misuse, theft of any personally owned device brought to school. This includes any financial charges that may result from overages to the student's/family's wireless data plan.

8. Students have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Wi-Fi network.

Moniteau School District
Network and Internet Access

STUDENT CONSENT AND WAIVER

By signing this form, I agree to the following terms:

1. My use of the Moniteau School District's network must be consistent with the Moniteau School District's primary goals.

2. I will not use the Moniteau School District network for illegal purposes of any kind.

3. I will not use the Moniteau School District network to transmit threatening, obscene, or harassing materials. The district will not be held responsible if I participate in such activities.

4. I will not use the Moniteau School District network to interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, and using the network to make unauthorized entry to any other machine accessible via the network. I will print only to my local printer or to the printer designated by the teacher/school official.

5. It is assumed that information and resources accessible via the Moniteau School District network are private to the individuals and organizations which own or hold rights to those resources and information unless specifically stated otherwise by the owners or holders of rights. Therefore, I will not use the Moniteau School District network to access information or resources unless permission to do so has been granted by the owners or holders of rights to those resources or information.

6. The district or its employees shall not be liable for the loss, damage, misuse, theft of any personally owned device brought to school. This includes any financial charges that may result from overages to the student's/family's wireless data plan.

7. Students have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Wi-Fi network.

Student Name: _____ Student ID #: _____
(Please Print Full Name)

Student Signature: _____ Grade: _____

Parent/Guardian: _____ Date: ____/____/____
(Please Print)

Parent/Guardian Signature: _____

Dear _____:

Congratulations and welcome to the Moniteau School District. We welcome you to our district and to service to the students and residents of the Moniteau Community.

As an employee of this district, you are required to be familiar with and follow rules and policies. The rules and policies have been established by the Board of School Directors, the state of Pennsylvania and the United States of America. In addition, your direct supervisor may have procedures/practices that directly affect your work.

The policies of the district, as established by the Board of School Directors, are available for review in the principal's office of each school building, the libraries of each school and the administration office. The Pennsylvania School Code is available in each school office and the administration center. The rules and policies of the state and federal governments are available from those agencies.

Some policies established by the Board of School Directors include:

- Internet/Email usage
- Criminal background checks
- Use of tobacco, alcohol or illegal drugs
- Proper interaction with students/peers
- Confidentiality
- Allocation of funds

These policies only represent a sampling of a comprehensive Policy Book established for the orderly operation of the school and safety of our past, present and future students. It is clearly understood that ignorance of any policy, law or procedure is not an excuse to violate the same. It is your responsibility to review this material, ask questions regarding this information and discuss this information with your supervisor. In the event your supervisor is not available, you have the right to contact the Superintendent to discuss this matter.

As a condition of employment, we ask that you carefully read the following statement, then sign and date where indicated. This letter will be placed in your personnel file.

I understand the Moniteau School District has established policies to direct the orderly operation of the district. I further understand that other laws have been established by the Commonwealth of Pennsylvania and the United States of America. This information was offered for my review. I understand that it is my responsibility to be familiar with these rules and policies and to follow these rules and policies as I fulfill my responsibilities to the school district, the students, my fellow workers and this community. I understand that failure to comply with these policies and rules will result in disciplinary action up to and including dismissal from duty. I have been offered the opportunity to review this letter and freely sign this form.

_____	_____	_____
Print Name	Sign Name	Date