Internet Safety and Acceptable Use for Network Access

2590.00

The Monticello School District provides access to the Monticello computer network and the Internet for students and staff to promote educational excellence by providing resource sharing, innovation and communication.

The purpose of education is to prepare students for life and work. In the world of work, students will encounter limited purpose networks. As part of the educational process, students should learn what conduct is inappropriate on a limited purpose network versus what is appropriate on a personal account. Staff should use the school's computer network in a way that is consistent with applicable District policies. Whoever uses the Monticello School District computer network (herein referred to as "the school network") and other instructional technology is expected to behave ethically and comply with District policy and administrative guidelines.

This District sets forth provisions in this policy to comply with the Children's Internet Protection Act (CIPA) and all federal requirements. The policy also addresses general network acceptable use for staff and students accessing the World Wide Web; software, graphics and other media for school use; storage space and for school related files; informational databases; and electronic communication with individuals both inside and outside the school network.

Responsibilities

Access to the Internet, school network and other instructional technology is an important learning resource. The opportunity of access must be utilized responsibly to maintain a positive learning environment and instructional access for all. These technologies rely on convenient communication and shared resources; therefore, individuals must be sensitive to the impact their actions may have on the learning community.

All students and staff will be informed of their rights and responsibilities as users of the school network prior to gaining access to that network, either as an individual user or as a member of a class or group. Individuals (and parents/guardians, if applicable) must complete an Electronic Resources User Agreement prior to obtaining access.

Because the Internet is a network with global reach, individuals may encounter materials that are not considered appropriate or suitable by parents and other members of the learning community. Acceptable use behaviors and safety policies are outlined below.

District staff and parents/guardians are responsible for conveying and discussing responsible technology use with their students and children. In accordance with federal law, the staff is responsible for monitoring student use of the Internet while in their classrooms. Parents and guardians bear the responsibility for supervision of internet and technology use outside of school.

Staff will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district curriculum. The basics of safe online behavior will be covered through district curriculum and in cooperation with law enforcement to include the appropriate interaction with other individuals on social networking websites and in chat rooms, and the dangers of cyber bullying.

As much as possible, access to district information resources will be designed in ways which point students to those which have been reviewed and evaluated prior to use. While students may be able to move beyond those resources to others which have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives.

School Network, Internet and Instructional Technology
Terms and Conditions of Use

1. Acceptable Use

1.1 The Monticello School District has established the computer network and other instructional technologies for a "limited educational purpose," which includes classroom activities, career development, research and teacher-approved self-discovery activities.

1.2 The use of these resources must be in support of education and research consistent with the education and research objectives of the Monticello School District. Downloading or using the network to access music files, games, or video is not allowed without the express permission of a teacher or administrator who has evaluated the educational purpose of such actions.

1.3 Transmission of any material in violation of national or state regulation is prohibited. This includes, but is not limited to, copyrighted, harassing, threatening, discriminatory or obscene material.

1.4 Pirating, which is the illegal copying or selling of software or copyrighted material, is prohibited.

1.5 Accessing social networking sites not expressly approved by administration is prohibited.

1.6 Hacking or attempting to compromise the security of either the school network or any external network is prohibited. This includes downloading files that could subvert existing security measures.

1.7 Making repeated attempts to access blocked sites or accessing proxy sites to subvert the Internet filtering system is prohibited.

1.8 Users are prohibited from sharing passwords or trespassing in another's folders, work or files.

1.9 The intentional damage to computers and other electronic devices, computer systems or the school network is prohibited.

1.10 The District is not liable for any damage suffered by a user of the school network including, but not limited to, loss of data stored or transmitted by technology resources or through interruption of service. The District is not responsible for any mistakes, liability, copyright infringements or other costs incurred by the individual using the District technology resources, or the accuracy or quality of information received over technology resources.

1.11 Fundraising for political activities may not be conducted on the network.

1.12 The computer network is not for commercial purposes. Students may not purchase products or services via the network without permission of the principal. Staff may not use the network to offer or provide products or services of a commercial nature.

1.13 The District will comply with Wisconsin statutory requirements and administrative rules related to technology.

2. Technology Protection Measures

2.1 The District employs technology protection measures to protect students and other users from seeing inappropriate materials and prevent unauthorized individuals from gaining access to the school network.

2.2 The District shall filter websites that contain obscenity, pornography, other materials that may be harmful to minors and those sites that interfere with the educational objectives of the school or make excessive demands on the network.

2.3 The web filter database shall automatically download updates to keep protection as current as possible. The technical staff shall be able to open and close sites as needed for instructional purposes.

2.4 Filtering shall be effective throughout the entire network.

2.5 The District takes measures to prevent computer viruses but users must share responsibility for keeping the school network secure. Suspicious emails or attachments should be reported to the network administrator immediately. The loading or creation of computer viruses is also prohibited. Any user with knowledge of such activity should be promptly reported to administration for further action.

2.6 The District shall utilize firewall technologies to assist in preventing unauthorized access.

2.7 The District has the capability to monitor Internet access and may check on an individual's record of access.

3 Limitations, Privileges and Privacy

3.1 The Use of the Internet and all technology resources is a privilege, not a right, and inappropriate use may result in a cancellation of technology privileges, legal action, and discipline up to and including suspension and expulsion for students and discipline up to and including discharge for employees.

3.2 Users should have no expectation of privacy in the contents of any communications or files on District technology resources unless such expectation is granted by law. The District maintains the right to access, inspect, investigate and monitor its resources, including all files, communications and information created on, with, or transmitted using its technology resources without notice to or consent of the user.

3.3 The District provides information and training in proper use of the network. That instruction may include additional guidelines not mentioned in this policy.

3.4 The District may examine computers and other electronic devices and search their contents if there is a reason to believe school policies, rules or regulations have been violated.

3.5 Users may bring personal devices into the District to access the school network. Personal devices may include laptop computers, portable digital assistants (PDA's), cell phones, iPods/MP3 players, wireless devices, digital cameras, storage devices or other electronics. The District is not liable for the loss, damage or misuse of any personal device including while on District property

or while attending school-sponsored activities. The District is also not responsible for any mobile charges incurred as a result of using mobile access on devices similar to cell phones. Individuals who make use of any personal technology must follow all rules and guidelines of this policy and related policies, guidelines and rules.

3.6 Files in individual, unshared student folders should not be viewed by other students. Files in individual, unshared staff folders should not be viewed by other staff, with the exception of the system administrator, technical personnel and supervisors.

3.7 The District prohibits the unauthorized disclosure, use and dissemination of personal identification information regarding minors.

3.8 The District retains control of all data stored on all district-owned servers and devices and may exercise this control to monitor compliance with this policy.

4. Consequences for Violations of the Acceptable Use Policy

4.1 Violation of any provision of the Acceptable Use Policy may lead to termination of access at the discretion of administration. The length of time access will be denied will be based on the frequency of the violation, severity of the infraction.

4.2 Individuals may be subject to action under existing Board of Education Policies, school rules, handbooks and contractual agreements.

4.3 Student violations will be reported to parents/guardians.

4.4 Termination of access does not prohibit the District from pursuing or implementing other disciplinary measures.

A. Acceptable Use Violations that are severe or repeated may result in additional sanctions beyond termination up to, and including, expulsion (students) and dismissal (staff).

B. The District will contact local, state or federal authorities if there is any suspicion of illegal activity. The District will lawfully cooperate with local, state or federal officials in any investigation concerning illegal activities conducted through the school network.

5. The Monticello School District makes no warranties of any kind, whether expressed or implied, for the service it is providing.

5.1 The District will not be liable for any damages you suffer. This includes loss of data from delays, non-deliveries, mis-deliveries or service interruptions caused by District actions or your own errors or omissions.

5.2 The District is not responsible for any costs, liabilities or damages caused by the way you use the computer network.

5.3 The use of any information obtained via the Internet is at your own risk.

5.4 The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Legal References:	Children's Internet Protection Act Broadband Data Improvement Act of 2008 Section 947.0125 Wisconsin State Statutes – Unlawful Use of Computerized Communication Systems
Cross References:	2593.00, Locker Room Privacy 2590.01, Student Acceptable Use Agreement 2590.02, Employee Acceptable Use Agreement 3211.00, Employee Use of Technology 5795.00, Cyber Bullying
Approved:	May 13, 1997
Revised:	February 9, 2005 March 12, 2008 January 14, 2009 July 8, 2009 July14, 2010 June 11, 2014