 **MINERAL POINT UNIFIED SCHOOL DISTRICT POLICY 443.7**

**ACCEPTABLE USE AND INTERNET SAFETY POLICY
FOR STUDENTS, STAFF AND GUESTS**

 The Mineral Point Unified School District has invested significantly in technology that offers vast, diverse and unique resources to students, staff and guests. The district’s goal in providing these services is to promote educational excellence by facilitating resource sharing, innovation and communication.

 The District supports access by students, staff and guests to rich information resources along with the development of appropriate skills to analyze and evaluate resources. In today’s world, access to and manipulation of information is a critical skill. Staff, students and guests will have available to them appropriate technological tools necessary to explore the world both from the inside and outside the classroom walls. The use of technology is a privilege, not a right, and appropriate conduct will result in revocation of those privileges.

 It is the policy of the Mineral Point Unified School District to:

a. prevent access over its network to inappropriate material via the Internet,
 electronic mail or other forms of direct electronic communications;

 b. prevent unauthorized access or unlawful online activity;

c. prevent unauthorized online disclosure, use or dissemination of personal
 identification information of minors; and

d. comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47
 USC 254 (h)].

**I. Technology Defined**

 A. School District Technology Devices

The use of technology that is owned or leased by the Mineral Point Unified School District is subject to the terms of this policy. Technology is defined under this policy as including, but not limited to the use of audio; video and computer software;

**Policy 443.7 Continued:**

computers; peripherals; network and communications equipment and related hardware; and video and audio equipment. District technology is to be used to enhance instruction, support learning and to develop professionally.

 B. Personal Technology Devices

The conditions set forth in this policy shall also apply to the use of laptop computers, net-book computers and other portable computing devices or accessories such as handheld computers, cell phones, PDAs, digital cameras, digital readers, music players, flash drives or other storage devices not owned by the Mineral Point Unified School District and brought into the school by students, parents, visitors or staff members.

 **II. Purpose**

 Despite its significant value, it is possible to encounter materials and interactions on the network that are not consistent with the educational goals of the district. It is the purpose of this policy to serve as a warning, provide guidelines for Internet safety and to identify examples of acceptable and unacceptable use of district technology and the Internet. Before the district provides network or Internet access, adult users and the parents/guardians of minor users must acknowledge their agreement to abide by this policy by submitting the accompanying signed agreement to the district.

 **III. Privacy**

 The district reserves the right to monitor, inspect, copy, review and store at any time, and without prior notice, any and all usage of the network and Internet access, and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the Mineral Point Unified School District and no user shall have any expectation of privacy regarding such materials.

The Mineral Point Unified School District reserves the right to inspect, at any time, any personally-owned device while connected to the district network whether by hard wire or wireless connection.

**Policy 443.7 Continued:**

 **IV. Internet Safety**

 All users are advised that access to the Internet includes the potential for access to materials that are inappropriate or harmful to minors. Every user (pupil and adult) must take responsibility for his or her use of the Internet and avoid sites and activities that are inappropriate or harmful to minors. Users who find sites that are inappropriate or harmful to minors shall report such sites to a designated official. Also, users who find other users visiting sites that are inappropriate or harmful to minors shall report such misuse to a designated official.

 It shall be the responsibility of the Mineral Point Unified School District staff to attempt to monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children’s Internet Protection Act. Furthermore, the district will educate students about Internet safety as part of the information technology courses, as well as instruction within the regular classrooms. The instruction will include appropriate use of social networking sites, communication tools, protection of personal information, and awareness of the dangers of cyber-bullying and sharing inappropriate images.

 Any adult staff member is considered a designated official for student reporting. Any administrator or supervisor is considered a designated official for adult reporting. Sanctions may include, but are not limited to, the loss of computer privileges, detention, suspension, separation or expulsion from school.

 The following Internet Safety guidelines along with the Acceptable and Unacceptable Use examples in sections V and VI serve as policy to be enforced by the district.

 A. Avoid material that is inappropriate or harmful to minors. By definition, this includes any text, audio segment, picture, image, graphic image file or other visual depiction that:

 \* Taken as a whole and with respect to minors, appeals to a crude
 interest in nudity, sex or excretion.

 \* Depicts, describes or represents, in an apparently offensive way with
 respect to what is suitable for minors, an actual or simulated sexual
 act or sexual contact, actual, simulated or perverted sexual acts, or an
 indecent exposure of the genitals.

**Policy 443.7 Continued:**

 \* Taken as a whole, lacks serious literary, artistic, political or scientific
 value to minors.

 B. Guard your personal safety. Users should not reveal personal information
 such as full name, home address, telephone number, credit card numbers or
 Social Security numbers. Minors should not arrange face-to-face meetings
 with someone they have “met” on the Internet without permission of their
 parent or guardian.

 C. “Hacking” and other illegal activities are prohibited. Using the district’s
 computer network and Internet access to gain or to attempt to gain
 unauthorized access to other computers or computer systems is prohibited.
 Also prohibited is any use that violates a municipal ordinance of state or
 federal law relating to copyright, trade secrets
 or the distribution of obscene or pornographic materials.

 D. Maintain the confidentiality of students. Personally identifiable information
 concerning students may not be disclosed or used in any way on the Internet
 without the permission of the adult student or a minor student’s parent or
 guardian.

 E. Install Active Restriction Measures. The district, either by itself or in
 combination with the Internet Service Provider, will utilize filtering software or
 other technologies to protect users from accessing visual depictions that are
 obscene, child pornography or harmful to minors. The district will also filter
 and 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 the Mineral Point Unified School District determines is
 inappropriate.

 **V. Acceptable Use**

 Examples of acceptable use include but are not limited to:

 \* Use consistent with the mission of the Mineral Point Unified School
 District.

 \* Use of technology for curriculum activities.

**Policy 443.7 Continued:**

 \* Use that encourages efficient, cooperative and creative methods to
 perform the user’s job duties or educational tasks.

 \* Use in support of education, research and professional development.

 \* Use that provides unique resources and collaborative projects with
 appropriate educational partners.

 \* Use for general communication.

 **VI. Unacceptable Use**

 Examples of unacceptable use include, but are not limited to:

 \* Accessing or sending inappropriate material and e-mail messages such
 as obscene or abusive language, harassing or threatening messages,
 visual depictions that are obscene, child pornography or material
 harmful to minors.

 \* Breaching security by sharing and/or using unauthorized passwords or
 working from network accounts that are not assigned to the user.

 \* Using the district system to engage in any illegal act, such as arranging
 for a drug sale or the purchase of alcohol, etc.

 \* Using district technology to violate copyright or piracy (illegal copying
 or selling of material) laws or sharing of student assignment files in
 violation of classroom cheating policies.

 \* Engaging in conduct while using e-mail or other electronic
 communication systems that is intended to frighten, intimidate,
 threaten, abuse, annoy, offend or harass another person. These
 actions are illegal.

 \* Unauthorized use of Internet chat rooms, social networking websites
 and non school issued e-mail accounts.

 \* Use that causes congestion and disruption of the network, such as
 spreading viruses and attaching excessively large files.

 \* Deliberate damage to any district technology.

**Policy 443.7 Continued:**

 \* Using and/or installing unauthorized software on district-owned
 equipment.

 \* Utilizing district technology for the production of non-school related
 materials unless authorized to do so.

 Student questions about what constitutes appropriate or inappropriate use of the network should be directed to the teacher, media specialist or principal.

 Staff questions about what constitutes appropriate or inappropriate use of the network should be directed to the district superintendent or district technology coordinator.

 **VII. Consequences**

 Student Violations: Any student user who violates this policy will lose network, e-mail and/or Internet privileges as stated below:

 1st Offense – Range: from a warning up to 90 school days.

 2nd Offense – Range: up to 180 school days

 3rd Offense – Range: up to permanent loss of privileges while enrolled at
 the school.

 Severe Offense – Whether a first, second or third offense, violations of a
severe nature may result in permanent denial of computer privileges.

 All penalties will be administered by school principals and are subject to review by the administrative team. In all cases, compensation for damages will be assessed.

 Employee Violations: Any staff or guest user who violates this policy will be subject to disciplinary actions that include one or more of the following: directive guidance, written reprimand, loss of user privileges, suspension without pay or discharge from employment.

 All penalties will be administered by the district administrator and are subject to review by the School Board. In all cases, compensation for damages will be assessed.

**Policy 443.7 Continued:**

 **VIII. Warranties and Indemnification**

 The Mineral Point Unified School District makes no warranties of any kind, either expressed or implied, in connection with its supplying of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages or costs (including attorney’s fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user’s use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for their use.

In the case of a user under 18, the parent(s) or guardian(s) agree to cooperate with the school in the event of the school’s initiating an investigation of a user’s use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the school district’s network.

 Legal Reference(s): Title XII Children’s Internet Protection Act
 Wisconsin Statutes: 118.125 Pupil Records
 118.13 Pupil Nondiscrimination
 943.70 Computer Crimes
 944.21 Obscene Material or
 Performance
 947.0125 Unlawful Use of
 Computerized
 Communication Systems
 947.013 Harassment
 PL 94-553, Federal Copyright Law
 Family Educational Rights & Privacy Act (20 USC 12329)

 Adopted: August 1996
 Revised: July 2010

**ACCEPTABLE USE AND INTERNET SAFETY POLICY
STUDENTS, STAFF AND GUEST AGREEMENT**

I have read, understand and agree to abide by the terms of the Acceptable Use and Internet Safety Policy of the Mineral Point Unified School District. Should I commit any violation or in any way misuse my access to the school district’s computer network, e-mail and/or Internet, I understand and agree that my access privilege may be revoked and school disciplinary and/or appropriate legal action may be taken against me.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 Student, Staff or Guest (print clearly) Home Phone \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 Student, Staff or Guest (signature) Date Address\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User check one: \_\_\_\_\_\_\_\_\_\_ I am 18 or older \_\_\_\_\_\_\_\_\_\_ I am under 18

If I am signing this policy when I am under 18, I understand that when I turn 18, this policy will continue to be in effect and I agree to abide by this policy.

 **Parent or Guardian Agreement
 To be read and signed by parents/guardians of students or guests who are under 18 year of age.**

As the parent or legal guardian of the above minor, I have read, understand and agree that my child or ward shall comply with the terms of the Mineral Point Unified School District’s Acceptable Use and Internet Safety Policy for the student’s access to the District’s computer network, e-mail, and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child’s or ward’s responsibility for abiding the policy. I am therefore, signing this policy and I will not hold responsible the school, the school district and the Internet provider for computer network, e-mail and Internet access against all claims, damages, losses and costs, of whatever kind, that may result from my child’s or ward’s use of his or her access to such networks or his or her violation of the foregoing policy. Further, I accept full responsibility for supervision of my child’s or ward’s use of his or her access if and when such access is not in the school setting. I hereby give permission for my child or ward to use an account authorized by the school district to success the district’s computer network,
e-mail and the Internet.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 Parent or Guardian (print clearly) Home Phone \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 Parent or Guardian (signature) Date Address\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_