

SCHOOL DISTRICT OF MAYVILLE

363-Rule

INTERNET SAFETY AND ACCEPTABLE USE RULES

A. ACCEPTABLE USES OF THE NETWORK

The District is providing access to its school computer systems, computer networks, and the Internet for educational purposes only. If a user has any doubt about whether a contemplated activity is educational, he/she may consult with the person(s) designated by the school to help them decide.

1. Students may access an Internet resource via District technology only with the proper consent of the teacher. The Internet is an extension of the classroom and teachers are responsible for and must be aware of where their students go on the Internet.
2. All users must abide by rules of Network etiquette - Netiquette, including being polite and using appropriate language and graphics.
3. All users must adhere to the copyright laws of the United States (U.S.C. 17) and the Congressional Guidelines that delineate it regarding software, authorship and copying information.
4. Images and school work products of K-12 students may be included on the website without identifying captions or names. Before posting a student's photo or school work on any school-related website, appropriate written consent must be obtained from the student's parent/guardian. Appropriate written consent means a signature by a parent or legal guardian of the student. Under no circumstances will K-12 student photos or work be identified with first and last name on a Mayville School District website, including the district, school or teacher website.
5. Any subscription to list serves, bulletin boards or online services must be approved by the District Administrator or his/her designee prior to any such usage.

Network and Internet access is provided as an educational tool. 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 computer 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 District and no user shall have any expectation of privacy regarding such information.

B. UNACCEPTABLE USES OF THE NETWORK include, but are not necessarily limited to:

1. Use of threatening, profane, harassing or abusive language. No swearing, vulgarities, suggestive, obscene, belligerent or threatening language is permitted. Avoid language and/or graphic representations which may be offensive to other users. Do not use network or Internet access to make, distribute or redistribute jokes, stories or other

material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion or sexual orientation.

2. Accessing pornographic or obscene materials, or other materials harmful to children.
3. Uses that cause harm to others or damage to property or jeopardizes network security. For example:
  - Do not engage in defamation (harming another's reputation by lies).
  - Do not disclose or share your password with others.
  - Do not invade the privacy of another user, use another's account, impersonate another user, post personal messages without the author's consent or send or post anonymous messages.
  - Do not assume that a sender of email is giving his/her permission to forward or redistribute the message to third parties or to give his/her email address to third parties. This should only be done with permission or when the user knows that the individual would have no objection.
  - Do not tamper with computer hardware or software.
  - Do not load or create a computer virus or load any software that destroys files and programs (e.g., Trojan horse, time bomb), confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.
  - Do not participate in hacking activities or any form of unauthorized access to other computers, networks or information systems.
  - Do not use anonymous proxies to get around content filtering.
4. Use of the network for any illegal activities. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
5. Use of the Internet for commercial, political, financial or religious purposes is prohibited. Violations shall be reported to a teacher or an administrator immediately. Students may not use the SCS or school network to sell or buy anything over the Internet.

### C. INTERNET SAFETY

1. Parents/Guardians and Users. Despite the efforts taken by the District to provide for supervision and filtering, 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 network and Internet and avoid these sites.
2. Personal Safety. In using the network and Internet, users should never give out private or confidential information about themselves or others on the Internet. Users should never arrange a face-to-face meeting with someone they "met" on the Internet without a parent/guardian's permission.
3. 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 or the

adult student. No personal addresses, phone numbers or last names of students will be permitted to be given out on the Internet.

4. Active Restriction Measures/Online Monitoring. The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. As noted above, the use of anonymous proxies to get around the content filter is strictly prohibited and will be considered a violation of these rules. The school will also monitor the online activities of students, through direct observation and/or technological means.

#### D. VIOLATIONS/CONSEQUENCES

Use of the computer network and Internet is a privilege, not a right. A user who violates the District's Internet Safety and Acceptable Use Policy and Rules shall be subject to disciplinary action by the school administrator. Depending on the nature or severity of the violation, individuals may have their access to the district's computer network and the Internet restricted, suspended or terminated or be subject to other appropriate disciplinary actions, which may include restitution for damages or compensation for necessary network and/or computer restoration work by technicians. Repeated violation will be dealt with in a progressively more severe manner. Any violation of federal, state or local laws or ordinances will be in addition to district disciplinary action and will follow legal provisions as established by statute.

Student Violations:

Students are subject to the following:

**First Offense:** Immediate suspension from network use or access until a disciplinary conference is held with parent/guardian, student and school administration.

**Second Offense:** Depending on the nature or severity of the violation, individuals may have their access to the District's computer network and the Internet restricted, suspended or terminated or may be subject to other appropriate disciplinary actions.

APPROVED: April 5, 1999

REVISED: