ACCEPTABLE USE/INTERNET SAFETY POLICY FOR TECHNOLOGY

PURPOSE

The Fort Madison Community School District (hereinafter called the "FMCSD") promotes the use and development of electronic information resources as a means to support learning and to enhance instruction. The Internet allows students and staff to access significant educational material and opportunities. The FMCSD wishes to allow students and adults access to curriculum based information resources no matter where they may be. To this end, the district permits its students and adults to access the Internet.

The responsible use of district facilities is the overriding goal of this policy. The Internet can provide access to the most recent research and the most up-to-date statistics and opinions. However, the Internet can also provide access to controversial and offensive information. While it is in fact impossible to completely protect exposure to inappropriate materials, it is important that the district have acceptable use regulations to provide guidelines for the use of this vital informational resource. The FMCSD believes that the benefits of Internet access far outweigh the risks and that the key to safe Internet usage is based on education and example.

Copies of this policy and its administrative procedures will be made available to all district staff, its students, and their parents/guardians.

SCOPE

This policy applies to students, employees, contractors, consultants, volunteers, temporaries, and other workers at the FMCSD, including all personnel affiliated with third parties all of which are considered users for the purposes of this policy. This policy applies to all equipment that is owned or leased by the FMCSD.

GENERAL GUIDELINES

Internet access is coordinated through a complex association of government agencies, regional and state networks, and commercial organizations. To ensure the efficient operation of the network, end users must adhere to established guidelines regarding proper conduct and efficient, ethical and legal usage.

Because the content on the Internet is hosted world-wide and not on district computers, students (and parents/guardians of the student, if the user is under 18 years old) should understand that some of the information available may be controversial and/or offensive. The FMCSD does not condone the use of such materials.

DEFINITIONS

Key terms are defined in the Children's Internet Protection Act.

RESOURCE LIMITS - The district is the owner of the technology and the decision maker regarding acceptable use. This system will only be used for educational and career development activities and limited, high-quality self-discovery activities. Users will not use the system for any products and/or service advertisement, commercial use or political lobbying, govern by state law. You will not post chain letters or engage in "spamming" (the sending of an annoying or unnecessary message to a large number of people). Student use of electronic mail, instant messaging, chat rooms, and other forms of direct electronic communications may be denied to individuals or a group of users. Unauthorized access, including so-called "hacking," and other unlawful activities are strictly prohibited by all online users.

SYSTEM MAINTENANCE - This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

SYSTEM SECURITY - Inappropriate use of the system is prohibited. System security is a high priority, if you find a security problem, you must notify your teacher or the system administrator. Do not demonstrate the problem to others. Electronic footprints are imprinted on the system whenever an action is performed. Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use your account. Do not give your password to another user. Do not trespass into another user's folders and files. Do not introduce or spread any computer virus which may destroy files or disrupt services.

EDUCATION, SUPERVISION AND MONITORING - It shall be the responsibility of all staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Subject to staff supervision, technology protection measures may be disabled or minimized only for bona fide research or other lawful purposes. FMCSD teachers will provide age-appropriate training for students who use Internet

connected computers. The training provided will be designed to promote FMCSD's commitment to:

a. the standards and acceptable use of Internet services as set forth in the agency's Internet Safety Policy;
b. student safety with regard to:
    i. safety on the Internet;
    ii. appropriate behavior while online, on social networking Web sites, and in chat rooms; and
    iii. cyberbullying awareness and response;
c. compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of FMCSD's acceptable use policies.

TECHNOLOGY PROTECTION MEASURE - To the extent practicable, the technology to prohibit access is visual depictions deemed obscene as defined in Section 1460 of Title 18, United States Code), child pornography (as defined in Section 2256 of Title 18, United States Code), or harmful to minors shall be used. The term "harmful to minors" means any graphic image file, or other visual 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 (as defined in Section 2246 of Title 18, United States Code), actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

INAPPROPRIATE LANGUAGE (Network Etiquette) - School use of the Internet is under the direct supervision of school staff, students are obligated to use it appropriately. Users should conduct themselves responsibly, ethically, and politely while online. Students and teachers are expected to conduct themselves in a socially acceptable manner at all times while on the Internet. All users are expected not to access, distribute, or redistribute jokes, stories, and other material which is based upon slurs or stereotypes relating to age, color, creed, national origin, race, religion, marital status, sex, sexual orientation, gender identity, physical attributes, physical or mental ability or disability, ancestry, political party preference, political belief, socioeconomic status, or family status.

LIMITATION OF LIABILITY - The district makes no warranties of any kind, either express or implied, that the functions of services provided by or through the system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. All users are advised to backup their personal data. The student and parent will not hold the teacher, school, or district liable for any materials retrieved from the Internet. The district will not be responsible for financial obligations arising through the unauthorized use of the system. The district does not warrant the effectiveness of the technology protection measure. The privacy of the system users is limited.

VANDALISM AND REPAIR - Do not mistreat equipment. Do not attempt to "fix" any software, hardware, or system problem, or attempt to add to or delete any programming, software, files, or other components of a system. Contact the system administrator for such problems.

COPYRIGHT & PLAGIARISM - You will respect the rights of copyright owners. Teachers will preview materials and sites that they require/recommend students to access. It is the standard practice to request permission for use of any content found on or through the Internet. You will not plagiarize words that you find on the Internet.

PERSONAL SAFETY - The unauthorized disclosure, use, and dissemination of personal information regarding minors and adults is prohibited. Harassment and other related activities is prohibited. Do not meet someone new that you met on the Internet (i.e. a chat room). Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

ENFORCEMENT AND FAILURE TO FOLLOW POLICY – Failure to adhere to network policies and rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings. The district will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through this system. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another user to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. Any employee found to have violated this policy may be subject to disciplinary action, including the termination of employment.

ROLES AND RESPONSIBILITIES

School Board

1. Review and adopt a policy on Acceptable Use/Internet Safety of the district system.
2. Review and adopt informed consent forms for parents.

Superintendent

1. Coordinate the district system with other regional and state organizations, as needed.
2. Enforce the Acceptable Use/Internet Safety Policy.

Director of Technology

1. Perform system maintenance to ensure system security.
2. Enforce the Acceptable Use/Internet Safety Policy.

Principal

1. Coordinate the district system at the building level.
2. Review the Acceptable Use/Internet Safety Policy with staff and ensure compliance.
3. Provide parents with informed consent forms.
4. Maintain user agreements.
5. Ensure proper training.
6. Ensure adequate student supervision.
7. Conduct building level activities (such as WWW Homepages).

Teacher

1. Review the Acceptable Use/Internet Safety Policy and ensure compliance.
2. Review school regulation and comply.
3. Provide age-appropriate training for students who use the Internet and review student responsibilities if necessary with students before Internet access is used.
4. Provide students with an appropriate level of supervision to ensure that the district Acceptable Use/Internet Safety guidelines are followed.
5. Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Do not give your password to another user. Do not trespass into another user's folders and files. Do not introduce or spread any computer virus which may destroy files or disrupt services.
6. Staff must properly log out at the end of their session.

Parent/Guardian

1. Be aware of the consequences set out by the school and the district for

unacceptable and inappropriate use.

2. Sign the informed consent form and understand compliance with this is a condition of access to district computer and electronic resources, and non-compliance may have other consequences as well.
3. Be aware of the risks inherent to Internet access while encouraging safe and acceptable practices of use.
4. Be aware that network storage areas may be treated like school lockers. For example, network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. User should not expect that files stored on district servers will be private.
5. Report misuse of the Internet to teacher or administrator.

Students

1. Sign the informed consent form and understand compliance with this is a condition of access to the district system and electronic resources, and non-compliance may have other consequences as well.
2. Conduct all activities in accordance with the guidelines and policies set out for the use of computer and electronic resources related to the school. Students will not access or explore online locations or material which are inappropriate for school assignments.
3. Conduct all activities in a responsible, ethical, legal, and courteous manner, especially when contacting others on the Internet. Students will be polite when corresponding with others. Abusive messages will not be tolerated. Use appropriate language.
4. Report misuse of the Internet to teacher or administrator.
5. Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Do not give your password to another user. Do not trespass into another user's folders and files. Do not introduce or spread any computer virus which may destroy files or disrupt services.
6. Students must properly log out at the end of their session.

Please note that Internet access is a privilege granted by the Fort Madison Community Schools. Abuse of the Acceptable Use/Internet Safety policy will lead to suspension and/or termination of the student's access to the Internet. This agreement shall remain in effect for the current school year unless terminated by either party by notification in writing. Failure to comply with these guidelines will result in the termination of network privileges for an individual or group.

Adopted: July 22, 1999
Amended: June 20, 2002; June 25, 2012
Reviewed: 2012, 2015
Legal Reference: Iowa Code § 279.8 (2009)