Board Policy

Code No. 603.14R1

STUDENT INTERNET/NETWORK APPROPRIATE USE REGULATION

Internet Access

I. Access to the Internet is available to all teachers and students as a source of information and a vehicle of communication.

II. Students will be able to access the Internet under teacher supervision (or other approved adult) to conduct curriculum-related research and communication.

A. Making Internet access available to students carries with it the potential that some students might encounter information that may not be appropriate for students. Although the Colfax-Mingo Community School District does employ an Internet filter, it is impossible to control all materials. Because information on the Internet appears, disappears, and changes, it is not possible to predict or control what students may locate.

B. It is a goal to allow teachers and students access to the rich opportunities on the Internet, while we protect the rights of students and parents who choose not to risk exposure to questionable material.

C. Student Internet records and access records are confidential records treated like other student records (see Board Policy #505.1 Student Records Access). Student work (art, writing, pictures) may be posted and credited on the district's web pages. Parent(s)/guardian(s) or students who choose not to have their name or work posted on a district web site must file a "Parental Authorization for Releasing Student Directory Information" form.

D. The smooth operation of the network relies upon the proper conduct of students and Staff members. Guidelines that require efficient, ethical and legal utilization of network resources must be observed. Utilization of these network resources should be limited to educational purposes.

E. Transmission of material, information, or software in violation of any district policy or regulation is prohibited.

F. The school district makes no guarantees as to the accuracy of information received on the Internet.

General Computing

I. Sharing your user ID with any other person is prohibited. In the event that you do share your user ID with another person, you will be responsible for the actions that other person appropriated.

II. Any unauthorized, deliberate action that damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

Network Security

I. Intentional attempts to "crash" network systems or programs are punishable disciplinary offenses.

II. Any attempts to secure a higher level of privilege on the local computer or network systems are punishable disciplinary offenses.

III. The willful introduction of computer "viruses" or other disruptive/destructive programs into the network or into external networks is prohibited.

IV. The possession of "hacking software" or visiting a "hacking" web site is prohibited.

V. Any attempt, including the use of proxy sites, to bypass the district Internet filtering system is prohibited.

VI. A personally owned computing device may not be connected to the district network without permission from a member of the District Technology Department; however limited Internet access may be available through the public wireless network.

Permission to Use Internet

Parents of students who do not wish to grant their student permission to use the Internet should use the District Internet Access Deny Form *(603.14E1)* to deny Internet access.

Student Use of Internet

I. Equal Opportunity

1. Internet shall be available to all students within the District. The amount of time available for each student may be limited by the number of available terminals and the demands for each terminal.

II. On-line Etiquette

1. The use of the network is a privilege. As a user of the Internet, students may be allowed access to other networks. It is the user's responsibility to abide by the policies and procedures of these other networks.

2. Students should adhere to on-line protocol:

a. Respect all copyright and license agreements.
b. Cite all quotes, references, and sources.
c. Only remain on the system long enough to get needed information; then exit the system.
d. Non-educational games are not permitted on school computers.
e. Students are not permitted to download music or other executable files without prior permission.
f. Apply the same privacy, ethical, and educational considerations utilized in other forms of communication.
g. Students are not permitted to stream audio or video unless instructed to do so be a staff member for the purpose of instruction.

3. Student access for electronic mail will be through the supervising teacher's account or class account at the elementary level. Middle school and high school students may be issued a school email account. Students should adhere to the following guidelines:

a. Others may be able to read or access your mail. Never send any messages of a private nature.
b. Delete unwanted messages immediately.
c. Use of objectionable language is prohibited.
d. Always sign your name to messages.
e. Electronic mail should only be utilized for educational purposes.

4. Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.

a. Recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
b. Never agree to meet someone they meet online in real life without parental permission.
c. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher, or staff if you're at school; parent if you're using the device at home) immediately.

5. Cyberbullying will not be tolerated.

a. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying.
b. Don't be mean.
c. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.
d. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges.
e. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

III. Restricted Material

Students shall not intentionally access or download any text file or picture, or engage in any conference that includes pornography. Also, students shall not intentionally access or download any text file or picture, or engage in any conference that advocates violence, racism, anarchy, treason or discrimination.

IV. Unauthorized Costs

If a student gains access to any service via the Internet which has a cost involved, the Colfax-Mingo Community School District will not be responsible for those costs. The student accessing such a service will be responsible for those costs.

V. Personal Computers

Personal computers or other network devices will not be permitted access to the District network without prior knowledge of the Director of Technology; however, limited Internet access may be available through the district Public Wireless Network.

Examples of Acceptable Use
I will:

a. **Use school technologies for school-related activities.**
b. **Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.**
c. **Treat school resources carefully, and alert staff if there is any problem with their operation.**
d. **Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.**
e. **Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.**
f. **Use school technologies at appropriate times, in approved places, for educational pursuits.**
g. **Cite sources when using online sites and resources for research.**
h. **Recognize that use of school technologies is a privilege and treat it as such.**
i. **Be cautious to protect the safety of myself and others.**
j. **Help to protect the security of school resources.**

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use
I will not:

a. Use school technologies in a way that could be personally or physically harmful.
b. Attempt to find inappropriate images or content.
c. Engage in cyberbullying, harassment, or disrespectful conduct toward others.
d. Try to find ways to circumvent the school's safety measures and filtering tools.
e. Use school technologies to send spam or chain mail.
f. Plagiarize content I find online.
g. Post personally-identifying information, about myself or others.
h. Agree to meet someone I meet online in real life.
i. Use language online that would be unacceptable in the classroom.
j. Use school technologies for illegal activities or to pursue information on such activities.
k. Attempt to hack or access sites, servers, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

<u>Student Violations; Consequences and Notifications:</u>

Students who access restricted items on the Internet shall be subject to the appropriate action described in the school's discipline policy handbook OR to the following consequences:

I. First Offense

Any Student who inappropriately uses the district network, computers, or accesses restricted sites on the Internet shall lose network and/or Internet access for up to 18 weeks at the discretion of a building administrator. Parents will be notified of this offense.

II. Second Offense

On the second violation of inappropriate use of the district network, computers, or access of restricted sites on the Internet during a school year the student shall forfeit all network and/or Internet privileges for the balance of the school year or at least a period of 18 weeks.

III. In certain situations, because of the serious nature of the violation of this policy, all internet privileges may be denied.

IV. Violation of other District disciplinary policies through the misuse of the Internet will result in sanctions called for in those policies.

Date of Adoption:
August 18, 2014 Board Policy
Code No. 603.14R1