

MARION CENTER AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: INTERNET SAFETY

ADOPTED: February 27, 2006

REVISED:

815.1. INTERNET SAFETY	
<p>1. Purpose</p>	<p>The district has an obligation to ensure student safety and to balance this with the need for open communications when using the Internet. There are documented instances of students being inappropriately identified via the Internet and becoming subjected to unhealthy situations or unwelcome communications.</p>
<p>2. Authority P.L. 106-554 Sec. 1711, 1721, 1732</p>	<p>Technology Protection Measure. The Marion Center Area School District uses specific technology that blocks and/or filters Internet access. This technology protects both adults and minors against access to visual depictions that are obscene, child pornography, or harmful to minors.</p>
<p>3. Guidelines Pol. 218, 218.2, 248, 348, 448, 548, 815</p>	<p>Students shall have access to the resources of the network and the Internet so long as they comply with rules and restrictions established by this policy and implemented by the district. The use of computers, the network, or the Internet for illegal, inappropriate or unethical purposes by students and staff is prohibited and will be sanctioned in accordance with related district policies on harassment and discipline. Specifically, but not limited to, the following are prohibited:</p> <ol style="list-style-type: none"> 1. Use to facilitate illegal activity. 2. Access to inappropriate matter on the Internet. 3. Sending or displaying offensive messages or pictures. 4. Using obscene language. 5. Harassing, insulting or attacking others. 6. Damaging computers, computer systems, or networks. 7. Using electronic mail, chat rooms, and other forms of district communication that would violate the safety and security of minors. 8. Violating copyright laws.

9. Unauthorized access, including so-called "hacking" and other unlawful online activities.
10. Unauthorized disclosure, use and dissemination of personal information regarding minors.
11. Use for commercial or for-profit purposes.
12. Use for non-work or non-educational related communications.
13. Use for product advertisement.
14. Use to develop programs that harass other users or to infiltrate a computer system and or damage the software components of a computer.
15. Use to post or distribute information that is harmful or prejudicial: for example, materials that are libelous and obscene as defined by the law of the Commonwealth of Pennsylvania or the United States.
16. Use to transmit material determined by the administration to be offensive or objectionable.
17. Use to intentionally obtain or modify files, passwords or data belonging to other users.
18. Use to represent other users on the network.
19. Hate mail, harassment, discriminatory remarks, and other antisocial communications.
20. The illegal installation, distribution, reproduction, or use of copyrighted software.
21. The loading or use of unauthorized games, programs, files or other electronic media.
22. Information deemed to be confidential shall not be disseminated on the district network or Internet.
23. Unauthorized participation by any user in MUDs (Multi-User Domains), MOOs (Multi-Oriented Objects), and game playing.

The above list is meant to serve as an example of activities the district considers prohibited. The district reserves the right to determine if any other activity, not appearing in the above list, constitutes an unacceptable use of the technology resources. The district further reserves the right to take such disciplinary action or formal legal action, civil or criminal as the situation may warrant enforcing the nature and intent of this policy.

Students may be granted e-mail access only through a teacher's account or a classroom account for educational purposes.

Students will not post personal contact information about themselves or others. Personal contact information includes home address or telephone number, work address or telephone number, age, gender, ethnicity, etc.

Students will not agree to meet with someone they meet or communicated with online.

Students will promptly disclose to their teacher or other school employee any web sites, e-mail message, or other information revealed to them that they believe to be inappropriate, or which makes them feel uncomfortable.

If the administration and staff wish to publish student work on the Internet, the following guidelines need to be followed:

1. Only first names are used in published student work.
2. Pictures that are a part of student publishing should not include identifying information.
3. Under no circumstances should a student's home address or phone number be included.
4. If replies to published student work are appropriate, the sponsoring teacher's address should be the e-mail address displayed, not the student's personal e-mail address.
5. In special circumstances with parental-signed release, identifying information can be added.

6. If special circumstances make it appropriate for older students to provide identifying information along with published work (one example might be college entrance or employment opportunities that would be enhanced by viewing a student's work online), the student and the supervising staff member must carefully weigh the potential for risk against the perceived advantage of posting this identifying information. Students must seek guidance and approval from school staff and must have written parental consent in instances where there is uncertainty before posting identifying information.

Any parent/guardian wishing to deny their child's access to the internet shall do so in writing to the building principal. The principal shall keep the letter on file and inform appropriate staff of the existence of such letter.

The Board reserves the right to make determinations of whether specific uses of computers, the network, or access to the Internet are consistent with this policy.