7540.03 - STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Students are encouraged to use Marcellus Community School's computers/network and Internet connection for educational purposes. Use of such resources is a privilege, not a right. Students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing the Internet at school, students must sign the Student Network and Internet Acceptable Use and Safety Agreement Form. Parent permission is required for minors.

Smooth operation of Marcellus Community School's Network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Students are responsible for their behavior and communication on the Internet. All use of the Network must be consistent with the educational mission and goals of the District.

B. Students may only access the Internet by using their assigned Internet account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their passwords. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers when leaving them unattended.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network. Students may not intentionally disable any security features of the Network.

D. Students may not use the Internet to engage in "hacking" or other unlawful activities.
   1. Students shall not use the Network to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a wireless communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.
   2. Use of the Network to engage in cyberbullying is prohibited. "Cyberbullying" is defined as the use of information and communication technologies (such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal websites, and defamatory online personal polling websites), to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http//www.cyberbullying.ca)] Cyberbullying includes, but is not limited to the following:

   a. posting slurs or rumors or other disparaging remarks about a student on a website or on weblog;
   b. sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

c. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;
d. posting misleading or fake photographs of students on websites.

E. Transmission of any material in violation of any State or Federal law or regulation or Board policy is prohibited.

F. Any use of the Internet for commercial purposes, advertising, or political lobbying is prohibited.

G. Students are expected to abide by the following generally-accepted rules of network etiquette:

1. Be polite courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's computers/network. Do not use obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.
2. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet.
3. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.
4. Never agree to get together with someone you “meet” on-line without prior parent approval.
5. Check e-mail frequently and delete e-mail promptly from the personal mail directory to avoid excessive use of the electronic mail disk space.
6. Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by a staff member.

H. Use of Internet to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that 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, actual or stimulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the district’s computers/network (e.g., viruses) are also prohibited.

I. Malicious use of the Network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not engage in vandalism or use the Network in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify the teacher, building principal, or the Director of Technology if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain

access (hacking).

J. All communications and information accessible via the Internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto district hard drives is prohibited; all downloads must be to floppy disk or USB flash drive. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects the Network with a virus and causes damage, the student will be liable for any and all repair costs to make the Network once again fully operational.

L. Students must secure prior approval from a teacher or the Director of Technology before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or "Listservs."

M. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (other than e-mail) without prior approval from a teacher or the principal. All such authorized communications must comply with these guidelines.

N. Privacy in communication over the Internet and the Network is not guaranteed. To ensure compliance with these guidelines, Marcellus School District personnel reserves the right to monitor, review, and inspect any directories, files and/or messages residing on or sent using the district's computers/network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

   Users have no right or expectation to privacy when using the Network. The district reserves the right to access and inspect any facet of the Network, including, but not limited to, computers, devices, networks or Internet connections, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

   A student's use of the Network constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the Network and related storage medium and equipment.

   Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated Marcellus School District policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated district policy and/or law, or if requested by local, State or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's files, e-mails and records.

O. Use of the Internet and any information procured from the Internet is at the student's own risk. Marcellus School District is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. Marcellus School District is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects should be cited the same as references to printed materials.

P. Disclosure, use and/or dissemination of personal identification information of minors via the Internet is prohibited, except as expressly authorized by the minor student's

parent/guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form.

Q. It shall be the responsibility of all members of the Marcellus Community School district staff to educate, supervise and monitor appropriate 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.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of building principals, technology department or designated representatives.

Teachers in each building or designated representatives will provide age-appropriate training for students who use Marcellus Community School District's Internet facilities. The training provided will be designed to promote Marcellus School District's commitment to:

a. The standards and acceptable use of Internet services as set forth in the Marcellus School District 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").

R. Any individual who is aware of a violation of the Board policy or this guideline, including inappropriate on-line contact, content, or conduct, such as sexting, harassment or cyberbullying, should bring it to the attention of their teacher or school principal immediately.

S. Proprietary rights in the design of web sites hosted on the district servers remains at all times with the district.

P.L. 106-554, Children's Internet Protection Act of 2000
P.L. 110-385, Title II, Protecting Children in the 21st Century Act
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

This Internet Safety Policy was adopted by the Marcellus Community School Board at a public meeting, following a normal public notice, on June 11, 2012.