Newaygo County Regional Educational Service Agency
4747 W. 48th Street
Fremont, MI 49412
(231) 924-0381

Computer Network **Board Policy 4510**
(Cf. 4520)

The Board authorizes the Superintendent or designee to develop services linking computers within and between buildings in the Agency, and to provide access to the international computer network (Internet) for students, staff and, if requested, members of the Board of Education. All computer network implementation shall be in line with the Board policy on technology and the Agency's educational goals.

Use of the computer network(s) as a part of any class or school assignment shall be consistent with the curriculum adopted by the Agency. The Agency's general rules for behavior and communications shall apply when using any computer equipment.

Individual Accounts

The Board authorizes the Superintendent or designee to provide individual accounts for students, staff, and, if requested, members of the Board, and access to the Agency computer network and the Internet, including electronic mail and file server space for developing and publishing material on the world wide web or other networked computer media. Such access shall be provided in furtherance of the Agency's educational mission, to enhance student knowledge and familiarity with technology, and to facilitate communication, innovation, and sharing of resources. To ensure the integrity of the educational process and to guard the reputation of the Agency, student and staff expression in public electronic media provided by the school may be subject to review, comment, editing, and/or removal by school officials.

Individual accounts and all use of Agency computer resources are considered a privilege, not a right, and are subject to the Agency's rules and policies. Electronic communications and stored material may be monitored or read by school officials. Electronic mail in individual accounts will not generally be inspected by school officials without the consent of the sender or a recipient, except as required to investigate complaints, which allege a violation of the Agency's rules and policies, or to investigate suspected misuse.

Student electronic mail and electronic storage space, which does not contain material made public by the student, shall be subject to the Agency's policy and rules on student records.

A fee may be charged by the Agency to defray the cost of individual accounts. However, if use of individual accounts is required for a core curricular class, no fees may be charged of a student for the duration of that class.

Privacy

The School Agency may collect and store Personally Identifiable Information (PII). In the event PII is collected, all information shall be secured in accordance with Board policies 5180 - Unauthorized Release of Information and 8940 - Student Records.

System Integrity

The Superintendent shall designate person(s) trained in computer technology ("system administrators") at the building and/or Agency level to implement the Agency's rules and regulations and to provide computer support for students, staff, and Board members. The Superintendent, in concert with the system administrators, shall employ hardware and software security to ensure the integrity of the system and to prevent unauthorized access to Agency and school records.

To preserve system integrity, employees shall use district issued equipment and/or software to access student and agency information. Use of personal devices is only permissible when accessing systems that are secured by agency issued credentials for the purpose of temporary or mobile access. Storage of agency or PII data on personal devices is not authorized.

Network Use

The Agency's network has not been established as a public access network. The Board has the right to place restrictions on its use to assure that use of the Agency's network is in accordance with its limited educational purpose. Use of the Agency's computers, network, and Internet services will be governed by this policy, related administrative regulations, the Student Code of Conduct, the staff tech use policy, and applicable employment contracts and collective bargaining agreements. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Network.

Users have no right or expectation to privacy when using the Network including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the Network.

The Superintendent or designee shall develop rules and procedures for computer and network use, and shall see to it that rules are published annually for students, parent(s)/guardian(s), staff, and Board members.

The Agency's computer network and public WiFi use rules shall be consistent with the following requirements:

- Users may not use Agency equipment to perform or solicit the performance of any activity that is prohibited by law.

- Users may not use the system (including social networking sites and chat rooms) to transmit or publish information that violates or infringes upon the rights of any other person, or information that is abusive, obscene, or sexually offensive, or considered to be cyberbullying or harmful to minors.

- Agency computer equipment shall not be used for commercial purposes by any user, or for advertisement or solicitation without prior written approval from the Superintendent.

- Except with prior authorization from a system administrator or the owner of the record in question, users may not access or attempt to access the records or files of other users, or of the Agency, nor delete, alter, or otherwise interfere with the integrity of computer-based information or resources.

- Users may not use the electronic mail facility to send unsolicited, bulk, chain, harassing, anonymous, or other messages which are an annoyance to the recipient or which may cause a degradation of system performance.

- Users may not use the network facility to access or bring into the school environment material that is inconsistent with the educational goals of the Agency, including but not limited to material which is defamatory, abusive, obscene, profane, sexually explicit, threatening, racially offensive, illegal, or which aids or advocates illegal activity other than non-violent civil disobedience.

Training and Education Programs

Staff members and students will be trained and educated respectively about Internet and Network use in accordance with the provisions of law and this policy. The training and education programs shall include:

A. safety and security of students while using email, chat rooms, social media and other forms or direct electronic communications;
B. the inherent danger of students disclosing personally identifiable information online;
C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying and other lawful or inappropriate activities by students or staff online, and
D. unauthorized disclosure, use, and dissemination of personal information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above, and staff members will monitor students' online activities while at school. Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Administrators are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. All Internet users are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Social Media (Cf. 5202)

Social media shall be defined as internet-based applications (such as Facebook, My Space, Moodle, other electronic blackboards, Twitter, etc.) that turn communication into interactive dialogue between users. The Board authorizes the instructional staff to access social media from the Agency's network, provided such access has an educational purpose for which the instructional staff member has the prior approval of the Administrator. However, personal access and use of social media, blogs, or chat rooms from the Agency's network is expressly prohibited and shall subject students *(optional) and staff members* to discipline in accordance with Board policy.

Agency Web Page(s)

Any and all Web pages representing the Agency shall be carried and posted only on the Agency's server and shall be designed and published in accordance with rules promulgated by the Superintendent.

Limiting Access

Pursuant to Federal law, the Board has implemented technology protection measures which block/filter Internet access to visual displays that are obscene, child pornography or harmful to

minors. The Board utilizes software and/or hardware to monitor online activity of students and staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. Nevertheless, parents/guardians are advised that a determined user may be able to gain access to services on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. Parents/Guardians assume risks by consenting to allow their child to participate in the use of the Internet. Parents/Guardians of minors are responsible for setting and conveying the standards that their children should follow when using the Internet. The Board supports and respects each family's right to decide whether to apply for independent student access to the Internet.

The technology protection measures may not be disabled at any time that students or staff members may be using the Network, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student or staff member who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or designee may disable the technology protection measure to enable access for bona fide research by staff members or other lawful purposes.

Complaints about content of networked information or access to blocked sites shall be handled in accord with the Agency's policy and procedures for complaints about library and instructional materials.

The Superintendent shall review the Computer Network policy and acceptable use policy and rules and recommend any changes, amendments or revisions to the Board as needed.

Approved: 5/7/07; 10/10/11; 8/13/12; 8/8/16
LEGAL REF: MCL 397.606; Protecting Children in the 21st Century Act, 47 U.S.C. § 254(h)(5)(B)