Ionia Public Schools
Bylaws & Policies

7540.04 - STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Advances in telecommunications and other related technologies have fundamentally altered the ways in which information is accessed, communicated, and transferred in society. Such changes are driving the need for educators to adapt their means and methods of instruction, and the way they approach student learning, to harness and utilize the vast, diverse, and unique resources available on the Internet. The Board of Education is pleased to provide Internet service to its staff. The Board encourages staff to utilize the Internet in order to promote educational excellence in our schools by providing them with the opportunity to develop the resource sharing, innovation, and communication skills and tools which will be essential to life and work in the 21st century. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources. The instructional use of the Internet will be guided by the Board's policy on Instructional Materials.

The District's Internet system has not been established as a public access service or a public forum. The Board has the right to place restrictions on its use to assure that use of the District's Internet system is in accord with its limited educational purpose. Staff use of the District's computers, network, and Internet services (Network) will be governed by this policy and the related administrative guidelines, and any 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 Internet is a global information and communication network that provides an incredible opportunity to bring previously unimaginable education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access up-to-date, highly relevant information that will enhance their learning and the education process. Further, the Internet provides students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

First, and foremost, the Board may not be able to technologically limit access to services through the Board's Internet connection to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, will open classrooms and students to electronic information resources which have not been screened by educators for use by students of various ages.

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 staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors.

The technology protection measures may not be disabled at any time that students 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 staff member who attempts to disable the technology protection measures will be subject to disciplinary action, up to and including termination.

The Superintendent or Director of Technology may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and

this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media and other forms of 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 unlawful 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.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. 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.

Staff members are responsible for good behavior on Board's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature.

Staff members shall not access social media for personal use on the District's network, and shall access social media for educational use only after submitting a plan for that educational use and securing the Principal's approval of that plan in advance.

General school rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines. Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the Board's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this policy and its accompanying guidelines.

Social Media Use

An employee's personal or private use of social media, such as Facebook, Twitter, MySpace, blogs, etc., may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy **8330**. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential employee information

may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to the use of the Network and the Internet for instructional purposes.

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)
47 C.F.R. 54.520

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY AGREEMENT

To access e-mail and/or the Internet at school, staff members must sign and return this form.

Use of the Internet is a privilege, not a right. The Board of Education's Internet connection is provided for business and educational purposes only. Unauthorized or inappropriate use will result in a cancellation of this privilege.

The Board has implemented technology protection measures, which protect against (e.g. block/filter) Internet access to visual displays/depictions/materials that are obscene, constitute child pornography, or are harmful to minors. The Board also monitors online activity of staff members in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. ( ) The Superintendent or _____ may disable the technology protection measures to enable access for bona fide research or other lawful purposes.

Staff members accessing the Internet through the Board's computers/network assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet.

The Board reserves the right, at any time, to access, monitor, review and inspect any directories, files and/or messages residing on or sent using the Board's computers/network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

( ) To the extent that proprietary rights in the design of a website hosted on the Board's servers would vest in a staff member upon creation, the staff member agrees to license the use of the website by the Board without further compensation.

Please complete the following information:

Staff Member's Full Name (please print): _____

School: _____

I have read and agree to abide by the Staff Network and Internet Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy is inappropriate and may constitute a criminal offense. As a user of the Board's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Staff Member's Signature: _____ Date: _____

The Superintendent is responsible for determining what is unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the Board's Staff Network and Internet Acceptable Use and Safety Policy and related Guidelines and take such other disciplinary action as is appropriate pursuant to the applicable collective bargaining agreement, State law and/or Board Policy.