7540.03 - STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

The District makes access to interconnected computer systems within the District as well as the Internet available to students to provide various means of accessing educational materials and opportunities.

The District's Internet system has a limited educational purpose and is not intended to serve as a public access service or a public forum. The District has the right to place restrictions on its use to assure that use of the District's computer system is in accord with its limited educational purpose. Student use of the District's computers, network and Internet services ("Network") will be governed by this policy, the related guidelines and the student disciplinary process.

The District encourages students to utilize the Internet to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The instructional use of the Internet will be guided by the District's policy on instructional materials.

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.

First, and foremost, the District may not be able to technologically limit access to services through the District's Internet connection to only those 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.

The District utilizes software and/or hardware to monitor online activity of students and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. 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 simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

At the discretion of the Superintendent, the Technology Protection Measure may be configured to protect against access to other material considered inappropriate for students to access. The Technology Protection Measure 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. The Superintendent or principal may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the Technology Protection measure. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the Technology Protection Measure. The Superintendent or principal may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Parents are advised that a determined user may be able to gain access to services on the Internet that the District 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 assume risks by consenting to allow their child to participate in the use of the Internet. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet. The District supports and respects each family's right to decide whether to apply for independent student access to the Internet.

The Superintendent is directed to prepare guidelines which address students' safety and security while using e-mail, chat rooms, instant messaging and other forms of direct electronic communications, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking") and other unlawful activities by minors online.

Network and Internet access is provided as a tool for your education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of electronic communications;

B. the dangers inherent with the online disclosure of personally identifiable information; and,

C. the consequences of unauthorized access (e.g., "hacking"), “cyber-bullying”, and other unlawful or inappropriate activities by students online.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The District expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. All Internet users (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Students and staff members are responsible for good behavior on the District'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. General school rules for behavior and communication apply. The District 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 District's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Administrative policy and its accompanying guidelines.

The District designates the Superintendent and principals as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of the Network.

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246

Updated 7-24-12

7540.03 - STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Students are encouraged to use the District'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 (see Sec. 943.70, Wis. Stat. (Computer Crimes) and Sec. 947.0125, Wis. Stat. (Unlawful Use of Computerized Communication Systems)). Prior to accessing the Internet at school, all students must sign the Student Network and Internet Acceptable Use and Safety Agreement. All students must also have the permission of his/her parent or guardian before accessing the Internet at school.

Smooth operation of the District'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.

B. Students may only access the Internet by using their assigned Internet/E-mail account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their passwords.

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.

D. Students may not use the Internet to engage in "hacking" or other unlawful activities. Possession of software and/or devices that are intended for “hacking”, bypassing District filters or any related equipment that would compromise District equipment while on premises is strictly prohibited.

E. Transmission of any material in violation of any State or Federal law or regulation, or District 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 District'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 and unless expressly authorized by your parent or guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form."

4. Never agree to get together with someone you "meet" on-line without prior parent approval.

5. Diligently delete old mail on a regular basis from the personal mail directory to avoid excessive use of the electronic mail disk space.

H. Use of the Internet to access, process, distribute, display, or print pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to students is prohibited. For example, 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.

To ensure that the District's computer resources are not used for inappropriate purposes and consistent with the Children's Internet Protection Act, the District has implemented technology protection measures on all computers with access to the Internet and World Wide Web that protect against access to visual depictions that are obscene, pornographic, and/or harmful to students. These measures are operating at all times, and enable the District to monitor and protect against access to the aforementioned visual depictions. We have additional and extensive systems and security mechanisms in place to ensure the security, integrity, and appropriateness of the data on our networks. We also rely on and respect each family's right to decide whether to allow their children access to the Internet and World Wide Web.

I. Malicious use of the District's computers/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 use the District's computers/network in such a way that would disrupt their use by others. Students must avoid intentionally wasting limited resources.

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 the District's hard drive must comply with the following:
- If a student downloads or transfers files, apps, plug-ins, etc. from the Internet, information services, and / or 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. Because of the vast amount of information, media and software that can be used or sent on the Internet, teachers are responsible for training students to make proper choices when doing research, downloading or uploading files and using online applications (i.e. video editing online). Teaching and learning time can be reduced by a large volume of internet activity. Staff and/or students should check the impact of large volume activities and relevancy of usage before using the Internet.

M. The District has software and systems in place that monitor and record all Internet, World Wide Web, and computer usage. The District wants users to be aware that security systems are capable of recording, for each and every user, each World Wide Web site visit, the amount of time spent actively using the World Wide Web, each chat, news group access, e-mail message, and every file transfer into and out of our internal networks to the Internet. No District student or employee should have any expectation of privacy as to his/her Internet or World Wide Web usage, or the privacy of any electronic mail message, file, download, note, or other data stored on or transmitted or received through any District computing facility. The District reserves the right to review computing activity and analyze usage patterns, and may choose to publicize this data to assure that the District's computing resources are devoted to maintaining the highest standards of educational benefit and employee productivity. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. The use of passwords does not guarantee confidentiality, and the District retains the right to access information in spite of a password.

N. Use of the Internet and any information procured from the Internet is at the student's own risk. The District is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The 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.

O. 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."

P. Proprietary rights in the design of web sites hosted on the District's servers remains at all times with the District.

943.70, Wis. Stats.
947.0125, Wis. Stats.
Family Educational Rights and Privacy Act of 1974, as amended
H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246