NORWALK PUBLIC SCHOOLS
NORWALK, CT
BOARD OF EDUCATION
NORWALK, CONNECTICUT

BOARD OF EDUCATION POLICY COMMITTEE

Committee Chairperson, Heidi Keyes

Tuesday, April 21, 2015
6 pm
Room A333
(City Hall – 3rd Floor)

AGENDA

1. Call to Order
2. Discussion: Outdoor Recess Guidelines (6142)
    i. Update and recommendations from NPS Recess Committee
3. Discussion: Information Technology Policies
    i. Development of "Bring Your Own Device" Policy (New)
    ii. Updates to Telecommunications/Internet -- Acceptable Use (6141.321), Computers: Websites/Pages (6141.322) , Internet Acceptable Use: Filtering (6141.323), Electronic Resources (6141.326)
4. Topics for May
5. Adjournment

6141.322

Instruction

Computers: Web Sites/Pages

The Board of Education allows the district and schools within the district to create and maintain Web sites for educational purposes. Web sites are avenues for educating, providing information, communicating and expressing creativity. District and individual school websites shall be used to share information about school curriculum and instruction, school-authorized activities, and other information relating to our schools and our mission. Websites shall also provide instructional resources for staff and students.

The content of materials published on websites should be professional quality and consistent with the education mission of the school system. Websites shall follow standards for ethical behavior in regard to information and technology by showing respect for the principles of intellectual freedom, intellectual property rights and the responsible use of information and technology. Pages shall reflect an understanding that both internal and external audiences will be viewing the information.

Any pages or links representing the school district shall follow guidelines and responsibilities pertaining to content standards, student records, copyright, and technical standards which are contained in the administrative regulations which accompany this policy.

(cf. 1110 - Communications with the Public)
(cf. 5125 - Student Records)
(cf. 5145.15 - Directory Information)
(cf. 5145.2 - Freedom of Speech/Expression)
(cf. 6141.321 - Acceptable Use of the Internet)
(cf. 6145.3 - Publications)
(cf. 6161.1 - Guidelines for Evaluation/Selection of Instructional Materials)
(cf. 6162.6 - Use of Copying Device, Copyrights)
(cf. 6163 - Instructional Resources for Students)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 (e) Access to Records of Minors.
Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.1232g.).
Dept. of Educ. 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. provisions act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et.seq
U.S. Const. Amend. I

Electronic Communications Privacy Act, 18 U.S.C. 2510-2522

Policy adopted:

6141.326

Instruction

Electronic Resources

The _____ Board of Education recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the _____ District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the District's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The District's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work and to take ownership of their lives.

The Board directs the Superintendent or his/her designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

(cf. 6162.6 – Copyrights)
(cf. 4118.4/4218.4 – E-Mail (Electronic Monitoring) (staff))
(cf. 4118.5/4218.5 – Staff Acceptable Computer Network Use)
(cf. 5125 – Student Records)
(cf. 5131.911 – Bullying)
(cf. 5131.913 – Cyberbullying)
(cf. 6141 – Curriculum Design/Development/Revision)
(cf. 6141.32 – Computer Literacy)
(cf. 6141.321 – Student Acceptable Use of the Internet)
(cf. 6141.322 – Websites/Pages)
(cf. 6141.323 – Internet Safety Policy/Filtering)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 (e) Access to Records of Minors.
53a-182b Harassment in the first degree: Class D felony. (as amended by PA 95-143)
Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).
18 USC § 25 10-2522 Electronic Communication Privacy Act
20 U.S.C. Section 6777, No Child Left Behind Act
20 U.S.C. 254 Children's Internet Protection Act of 2000
47 U.S.C. Children's Online Protection Act of 1998
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at

20 U.S.C.1232g.).
Dept. of Educ. 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. provisions act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et.seq.

Policy adopted:

6141.326

Instruction

Electronic Resources

K-12 Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support the Electronic Resources Policy of the Board of Education and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and with civility in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

Network

The District network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the District.

Acceptable network use by District students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Connection of staff personal laptops to the District network after checking with (insert title of position, i.e., technology director, IT director, assistant superintendent) to confirm that the laptop is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by district students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;

- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the (insert title of position);

- Support or opposition for ballot measures, candidates and any other political activity;

- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;

- Unauthorized access to other district computers, networks and information systems;

- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;

- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);

- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and

- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

Internet Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.

- Students and staff should not reveal personal information about another individual on any electronic medium.

- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.

- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;

- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are

prohibited: proxies, https, special ports, modifications to District browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;

- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering district e-mail boxes;

- The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to District computers;

- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and

- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security and Privacy

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- Change passwords according to District policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your user account password, keep it in a secure location;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen, or log off, if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy

The District provides the network system, e-mail and Internet access as a tool for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of Connecticut.

Disciplinary Action

All users of the District's electronic resources are required to comply with the District's policy and procedures [and agree to abide by the provisions set forth in the District's user agreement].

Violation of any of the conditions of use explained in the (District's user agreement), Electronic Resources Policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

(cf. 6162.6 – Copyrights)
(cf. 4118.4/4218.4 – E-Mail (Electronic Monitoring) (staff))
(cf. 4118.5/4218.5 – Staff Acceptable Computer Network Use)
(cf. 5125 – Student Records)
(cf. 5131.911 – Bullying)
(cf. 5131.913 – Cyberbullying)
(cf. 6141 – Curriculum Design/Development/Revision)
(cf. 6141.32 – Computer Literacy)
(cf. 6141.321 – Student Acceptable Use of the Internet)
(cf. 6141.322 – Websites/Pages)
(cf. 6141.323 – Internet Safety Policy/Filtering)

Legal Reference: Connecticut General Statutes
1-19(b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 (e) Access to Records of Minors.
53a-182b Harassment in the first degree: Class D felony. (as amended by PA 95-143)
Connecticut Public Records Administration Schedule V - Disposition of Education

Records (Revised 1983).
20 U.S.C. Section 6777, No Child Left Behind Act.
20 U.S.C. 254 Children's Internet Protection Act of 2000.
47 U.S.C. Children's Online Protection Act of 1998.
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.1232g).
Dept. of Educ. 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. provisions act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et.seq

Regulation approved

6141.321

Instruction

Telecommunications/Internet - Acceptable Use

The school district believes in the educational value of communications, the Internet, and electronic information services, and recognizes their potential to support its educational program, the curriculum and student learning. Resource sharing, communications, and innovation capabilities for both students and teachers have been increased with access to telecommunications and to the Internet. The district will make every effort to protect students and teachers from any misuses or abuses as a result of experience with an electronic information service. It is therefore imperative that members of the school community conduct themselves in a responsible, decent, ethical, and polite manner while using any network. Further, they must abide by all local, state and federal laws.

Guidelines for General Use

It is important to recognize that with increased access to computers and people all over the world also comes the availability of controversial material that may not be considered of educational value in the context of the school setting. Further, the school district recognizes the importance of each individual's judgment regarding appropriate conduct in maintaining a quality resource system. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in such judgment by providing the following guidelines.

1. All use of the Internet, electronic services or any telecommunications network must be support of educational objectives or research.

2. Any electronic mail accounts shall be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account.

3. All communications and information accessible via a network should be assumed to be private.

4. Any use of the district's computing resources or networks for illegal or inappropriate purposes accessing materials that are objectionable in a public school environment, or supporting such activities, is prohibited. Language that is deemed to be vulgar is also prohibited. Illegal activities shall be defined as a violation of the intended use of the service or network. Inappropriate use shall be defined as a violation of the intended use of the service or network. Objectionable is defined as materials that are identified as such by the rules and policies of the Board of Education that relate to curriculum materials and textbook adoption.

5. Any use of telecommunication opportunities for commercial purposes financial gain, product advertisement, political lobbying, or attempt to disrupt the use of the services by others, is prohibited.

6. The Board of Education has no control of the information on the Internet. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people.

7. Violations of the provisions stated in this policy may result in suspension or revocation of access privileges to the Internet, electronic services or district networks.

The Superintendent shall identify one administrator as the "District Internet Administrator" who will have responsibility for implementing this policy, establishing procedures, and supervising access privileges.

Guidelines for Student Use

Student use of electronic services is considered to be a privilege. Students at the elementary level may use telecommunications or the Internet only when supervised by a teacher or teacher aide. Guidelines for the use of these electronic services by elementary students will be developed by the District Internet Administrator.

Students in grades 6-12 who wish to use electronic services and networks that are available to them may do so provided that they:

1. Read and agree to the Acceptable Use Policy;
2. Sign Internet Use Agreement" (contract);
3. Obtain the signature of one parent/guardian (if under the age of 18) on the contract;
4. Have at least one teacher sign the contract form as a sponsor; and
5. Submit the completed contract to the designated person in each building.

Any parent or student who wishes to appeal any decision relative to Acceptable Use Policy should contact the District Internet Administrator.

Legal Reference: Connecticut General Statutes
51a-182b Harassment in the first degree: Class D Felony (as amended by PA 95-143)
20 U.S.C. Section 6777, No Child Left Behind Act
20 U.S.C. 254 Children's Internet Protection Act of 2000
47 U.S.C. Children's Online Protection Act of 1998

Policy adopted:

6141.321

Agreement

Instruction

Telecommunications/Internet - Acceptable Use

_____ PUBLIC SCHOOLS

_____, CONNECTICUT

Internet Use Agreement

Please read this document carefully before signing.

Internet access is now available to students and teachers in the School District.

The Board of Education is pleased to bring this access to _____ and believes the Internet offers vast, diverse, and unique resources to both students and teachers. Our goal in providing this service to teaches and students is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

1) electronic mail communication with people all over the world;

2) information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions;

3) public domain software and shareware of all type;

4) discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics; and

5) access to many University Library Catalogs, the Library of Congress and ERIC.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The School District has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. We firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a district user violates any of these provisions, his or her privileges/account will be terminated and future access could possibly be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

1) **Acceptable Use** - The purpose of the National Science Foundation Network (NSFNET), which is the backbone network to the Internet, is to support research and education in and among academic institutions in the United States by providing access to unique resources and the opportunity for collaborative work. The use of telecommunications/an electronic mail account must be in support of education and research and consistent with the educational objectives of the School District. Use of other organizations' networks or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to: copyrighted material threatening or obscene material, or material protected by trade secret. Use for commercial activities, product advertisement or political lobbying is prohibited.

2) **Privileges** - The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student who uses the Internet or who receives an account will be part of a discussion with a district faculty member pertaining to the proper use of the network.) System administrators will deem what is inappropriate use and the decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff may request the District Internet administrator to deny, revoke, or suspend specific user accounts.

3) **Network Etiquette** - You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

a. Be polite. Do not get abusive in your messages to others.

b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.

c. Do not reveal your personal address or phone number or those of students or colleagues.

d. Note that electronic (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in such a way that you would disrupt the use of the network by other users.

f. All communications and information accessible via the network should be assumed to be private property.

4) The School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages such as loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors or omissions. The district specifically denies any responsibility for the accuracy of quality of information obtained from the Internet.

5) **Security** - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator or your District Internet Administrator. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to Internet.

6) **Vandalism** - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses. If there is any cost involved in repairing such vandalism, the cost will be assumed by the parent/guardian or the student if he/she is 18 years or older.

_____ Public Schools

Internet Use Agreement

Internet access is now available to students and teachers in the School District.

The Board of Education is pleased to bring this access to _____ and believes the Internet offers vast, diverse, and unique resources to both students and teachers. Our goal in providing this service to teachers and students is to promote educational excellence in schools by facilitating resource sharing, innovation and communication.

STUDENT

I understand and will abide by the above Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.

_____

Student Signature *Date*

_____

School *Grade*

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the Internet Use Agreement. I understand that this access is designed for educational purposes. The School District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the district to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my child to access the Internet, to have an account and certify that the information contained on this form is correct.

_____

Parent or Guardian's Name (Please Print)

_____

Signature *Date*

SPONSORING TEACHER

I have read the Internet Use Agreement and agree to review this agreement with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student use of the network. As the sponsoring teacher, I do agree to instruct the student on acceptable use of the network and proper network etiquette.

_____

Teacher's Name (please print)

_____

Signature *Date:*

6141.323

Instruction

Internet Acceptable Use: Filtering

The _____ Public Schools is fortunate to have access to the Internet at all schools. This access provides increased opportunities for students and staff to conduct research and to communicate locally, nationally, and internationally.

This wonderful resource also provides access to material unsuitable for students and which has no educational value. It is the responsibility of all District staff to ensure that the Internet, as used in District Schools, is appropriately guided and monitored. Moreover, staff also has the responsibility to conduct themselves in an appropriate private manner when using the Internet.

Alternative/optional language to consider

The Board of Education provides computers, computer systems, software, electronic access privileges, and networks for students and staff to carry out the mission of the Board in an environment which ensures access to up-to-date information, management, and communication services. Responsible use of these systems and networks is expected of all students and staff.

The computers, computer systems, software, electronic access privileges, and networks are the property of the Board of Education and are to be used only for those activities directly related to teaching, learning, and/or management by students and staff. The equipment, infrastructure, and software are not to be used for personal gain by any student or staff member.

In order to ensure that the District's Internet connection is used in the appropriate manner and that all users are protected from any inappropriate information published on the Internet, the District has and is continuing to implement the following:

1. Professional development opportunities to help teachers integrate the use of the Internet into classroom teaching.

2. Use of the computers, computer systems, software electronic access privileges and networks shall be restricted to those users who have signed the District's "Acceptable Use Policy." In the case of minors, the "Acceptable Use Policy" must also be signed by the student's parent or guardian.

3. Implementation of a system developed to filter out Internet sites with content considered unacceptable for student viewing. A committee of teachers, parents, and administrators shall be used to receive appeals from users who have a specific use in mind for a filtered site.

The Internet changes rapidly making it impossible to filter all objectionable sites. Therefore, the staff role in supervising and monitoring student access to the Internet is critical. In addition, each individual has the responsibility to monitor their own navigation on the Internet to avoid undesirable sites.

Alternative/optional language to consider

Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to inappropriate material. Filtering should be used in conjunction with:

- *Educating students to be "Net-smart"*
- *Using recognized Internet gateways as a searching tool and/or homepage for students, in order to*

facilitate access to appropriate material;

- *Using "Acceptable Use Agreements;"*
- *Using behavior management practices for which Internet access privileges can be earned or lost; and*
- *Appropriate supervision, either in person and/or electronically.*

The placement of filters on District computers/computer systems is viewed as an exercise of the Board's ability to determine educational suitability of all material used in the schools.

Filters may be utilized with District schools to (1) block pre-selected sites, (2) block by word, (3) block entire categories like chat and newsgroups, and (4) through a pre-selected list of approved sites.

The Superintendent of Schools is directed to establish guidelines and procedures for responsible use of computers, computer systems, software, electronic access privileges, and networks provided by the Board of Education.

For Districts participating in the federal E-Rate program:

The District recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

(cf. 6141.321 - Acceptable Use of the Internet)
(cf. 6141.322 - Web Sites/Pages)

Legal Reference: Connecticut General Statutes

1-213 Access to public records. Exempt records.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.
46b-56 (e) Access to Records of Minors.
Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C. 1232g.).
Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)- parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
HR 4577, Fiscal 2001 Appropriations Law (contains Children's Internet Protection Act)
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.
Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21st Century Act
Reno v. ACLU, 521 U.S. 844 (1997)
Ginsberg v. New York, 390 U.S. 629, at 642, n.10 (1968)
Board of Education v. Pico, 457 U.S. 868 (1988)
Hazelwood School District v. Kuhlmeier, 484 U.S. 620, 267 (1988)

Policy adopted:

6141.323

Instruction

Internet Acceptable Use: Filtering

Preface

When minors are using the Internet, access to visual depictions that are obscene, child pornography or harmful to minors must be blocked or filtered. When adults are using the Internet, only material which is obscene or child pornography must be filtered or blocked.

Definitions

1. **Obscene** is to be determined by the following standards:

   - Whether the average person, applying contemporary community standards, would find the work, taken as a whole, appeals to the prurient interest;
   - Whether the work depicts sexual conduct in an offensive way; and
   - Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

2. **Child Pornography**, as defined in 18 U.S.C. 2256 means any visual depiction, including any photograph, film, video, picture, computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

   - the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
   - such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
   - such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
   - such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

3. Material **"Harmful to Minors"** is any picture, graphic image file or other visual depiction that:

   - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
   - depicts, describes, or represents, in a patently offensive way with respect to what is suitable to minors, an actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   - taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

Criteria for Filtering of Objectionable Sites

Anything that falls under at least one of the categories below shall/may be blocked/filtered. This list will be updated/modified as required.

Nudity/Pornography

- Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
- Provocative semi-nudity (e.g., lingerie models)
- Sites which contain pornography or links to pornographic sites
- **Exceptions:** Classical nudity (e.g., Michelangelo), swimsuit models

Sexuality

- Sites which contain material of a mature level (elementary/middle school levels)
- Images or descriptions of sexual aids
- Descriptions of sexual acts or techniques
- Sites which contain inappropriate personal ads

Violence

- Sites which promote violence
- Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
- Graphic autopsy or crime-scene images

Crime

- Information of performing criminal acts (e.g., drug or bomb making, computer "hacking")
- Illegal file archives (e.g., software piracy)

Drug Use

- Sites which promote the use of illegal drugs
- Material advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
- **Exceptions:** Material with valid educational use (e.g., drug-use statistics)

Tastelessness

- Images or descriptions of excretory acts (e.g., vomiting, urinating)
- Graphic medical images outside of a medical context
- **Exception:** Graphic medical images within a medical context

Language/Profanity

- Passages/Words too coarse to be softened by the word filter
- Profanity within images/sounds/multimedia files
- Adult humor; (e.g., inappropriate for the age/grade level of the persons accessing the material)

NOTE: The focus is on American English, but profanity in other languages or dialects is blocked if

brought to our attention.

Discrimination/Intolerance

- Material advocating discrimination (e.g., forms of intolerance and/or bigotry such as racial, goods, sexual orientation, disability, national origin, color or religious discrimination)
- Sites which promote intolerance, hate, or discrimination

Interactive Mail/Chat

- Sites which contain or allow inappropriate e-mail correspondence
- Sites which contain or allow inappropriate chat areas

Inappropriate Banner Acts

- Advertisements containing inappropriate images

Gambling

- Sites which allow or promote online gambling

Weapons

- Sites which promote illegal weapons
- Sites which promote the use of illegal weapons

Other Inappropriate Material

- Body modification: tattooing, branding, cutting, etc.

Judgment Calls

- Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

Procedures For Suggesting Site Be Blocked or Unblocked

If a District staff member observes a site which they believe to contain inappropriate material according to the criteria provided here, they may request that the site (URL) be blocked. Education Technology staff will review the site for inappropriateness. If the site meets the criteria for filtering, steps will be taken to block the site.

Disabling Blocking/Filtering Devices

The technology protection measures used to block or filter a site may or may not be disabled during use by an adult to enable access to bona fide research or other lawful purpose. (*NOTE: CIPA does not require schools or libraries to afford adults unfiltered Internet access.)*

There are no exceptions to the requirement that Internet access be blocked/filtered at all times for minors. If material has been wrongly blocked, it must be unblocked by the company providing the software, after a request has been made by the school or library.

Regulation approved:

6141.328

Instruction

Bring Your Own Device (BYOD) and Protocol for the Use of Technology in the Schools

As new technologies continue to change the world in which we live, they also provide many new and positive educational benefits for classroom instruction. To prepare students as 21st century thinkers and learners, students in the _____Public School District are now encouraged to bring their own technology to campus.

(Alternate language to the above paragraph)

(Alternate #1) **The Board of Education is committed to aiding students and staff in creating a 21st century learning environment. Therefore students and staff will be permitted to access the District's wireless network with their personal devices during the school day. With teacher approval, students may use their own devices to access the Internet and collaborate with other students.**

(Alternate #2) **Access to the District's wireless network, including the Internet shall be made available to students for instructional purposes in accordance with administrative regulations.**

(Alternate #3) **Technology use is everywhere in our world today. The Board of Education believes schools should play a role in teaching students to use technology appropriately. Rather than banning the devices the District's students use in their daily lives, the same devices they will soon come to rely on in their future professional lives, it is important to guide them in developing the skills needed to be productive digital citizens, by bringing their own technology to campus.**

Definition of "Device"

A "device" as part of this protocol is a piece of privately owned and/or portable electronic handheld technology that includes emerging mobile communication systems and smart technologies, laptops and netbooks, and any technology that can be used for wireless internet access, word processing, image capture/recording, sound recording and information transmitting, receiving, and storing.

(Alternate language to the above paragraph)

(Alternate #1) **For purposes of BYOD, a "device" means a privately owned wireless and/or portable electronic piece of equipment that includes laptops, netbooks, tablets/slates, iPod Touches, e-Readers, cell and smart phones.**

(Alternate #2) **For purposes of BYOD/BYOT a "device" means a privately owned wireless and/or portable electronic hand held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, portable internet devices, Personal Digital Assistants (PDAs), hand held entertainment systems or portable information technology systems that can be used for word processing, wireless internet access, image capture/recording, sound recording and information transmitting/receiving/storing.**

Internet

The only internet gateway that may be accessed while in the District Public Schools is the one provided by the District. Any device brought to the District will not be permitted to use outside internet sources.

Personal internet connective devices, such as but not limited to cell phones/cell network adapters, are not

permitted to be used to access outside internet sources at any time.

Software

Many software packages are now available as web browser applications. This negates the need to have required programs loaded onto student computers. Students can access what they will need through any web browser. Therefore, there is no required software necessary to take part in the Bring Your Own Device program.

Security and Damages

Responsibility to keep the device secure rests with the individual owner. The _____Public School District is not liable for any device stolen or damaged on campus. If a device is stolen or damaged, it will be handled through the administrative office as other personal items that are stolen or damaged. It is recommended that skins, decals, and other custom touches be used to identify physically a student's device from others. Additionally, protective cases for technology are encouraged.

Bring Your Own Device/Technology Student and Parent Agreement

The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his/her electronic device while at school. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole.

Students and parents/guardians participating in the Bring Your Own Device/Technology program must adhere to the Student Code of Conduct, as well as all applicable Board policies, particularly the Computer Acceptable Use policy.

The use of these devices, as with any personally owned device, is strictly up to the teacher.

(cf. 5114 – Suspension/Expulsion)
(cf. 5132.81 – Use of Electronic Devices)
(cf. 5131.911 – Bullying)
(cf. 5131.913 – Cyberbullying)
(cf. 5131 – Conduct)
(cf. 5144 – Discipline)
(cf. 6141.321 – Acceptable Computer Use Policy)
(cf. 6141.323 – Internet Acceptable Use: Filtering)
(cf. 6141.326 – Online Social Networking)

Legal Reference: Connecticut General Statutes
10-221 Boards of education to prescribe rules
Policy adopted:

6141.328

Instruction

Bring Your Own Device (BYOD) and Protocol for the Use of Technology in the Schools

The following guidelines shall govern the manner in which the Bring Your Own Device/Technology (BYOD/BYOT) policy and program are to operate within the District.

Readiness

The implementation of this program will require the support of a robust wireless infrastructure. A network

evaluation will be conducted to determine any and all necessary infrastructure changes and upgrades that are needed before a full implementation.

The implementation of the program may require minor changes in the manner network administration is currently done. Considerations must be given to issues of security, accessibility, cloud computing, etc. The readiness evaluation report must include any and all network administration changes needed to support BYOD/BYOT.

Definitions

A "device" as part of this protocol is a piece of privately owned and/or portable electronic handheld technology that includes emerging mobile communication systems and smart technologies, laptops and netbooks, and any technology that can be used for wireless internet access, word processing, image capture/recording, sound recording and information transmitting, receiving, and storing. (*Or use one of the alternative definitions found in the sample policy)*

Teachers' Role

1. Teachers are facilitators of instruction in their classrooms. Therefore, they will not spend time on fixing technical difficulties with students' personal devices in the classrooms. They will educate and provide guidance on how to use a device and troubleshoot simple issues, but they will not provide technical support. This responsibility resides at home with parents/guardians.

2. Teachers may communicate information regarding educational applications and suggest appropriate tools that can be downloaded to personal devices at home. Parents will need to assist their younger children with downloads if they wish to follow teachers' suggestions. No applications are to be downloaded at school.

3. Teachers are to closely supervise students to ensure appropriate use of technology in the classrooms.

4. It is understood that not every student has his/her own electronic device. To ensure equal accessibility to technology resources, teachers will provide students with technology available within the school.

5. The use of these student personal devices, as with any personally owned device, is strictly up to the teacher.

Security and Damages

1. The District, or any of its schools, is not liable for any device that is stolen or damaged. Responsibility to keep the device secure rests with the individual owner. If a device is stolen or damaged, it will be handled through the administrative office as other personal items are stolen or damaged. It is recommended that skins, decals, and other custom touches be used to identify physically a student's device from others. Additionally, protective cases for technology are encouraged.

2. Personal devices cannot be left on campus before or after school hours.

Operating Principles for Use of Personal Devices on School Campus

1. Devices cannot be used during assessments, unless otherwise directed by a teacher.

2. Students must immediately comply with teachers' requests to shut down devices or close the screen. Devices must be in silent mode and put away when asked by teachers.

3. Students are not permitted to transmit or post photographic images/videos of any person on campus

on public and/or social networking sites.

4. Personal devices must be charged prior to bringing them to school and run off their own batteries while at school.

5. To ensure appropriate network filters, students will only use the District's wireless BYOD/BYOT connection in school and will not attempt to bypass the network restrictions by using 3G or 4G network.

6. Students must be instructed that bringing devices on campus or infecting the network with a virus, Trojan, or program designed to damage, alter, destroy, alter, or provide access to unauthorized data or information is in violation of the District's Acceptable Use Policy and will result in disciplinary actions.

7. The District has the right to collect and examine any device that is suspected of causing problems or is the source of an attack or virus infection.

8. Students must be instructed that possessing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of the Acceptable Use Policy and will result in disciplinary actions.

9. Students can only access files on the computer or Internet sites which are relevant to the classroom curriculum and suggested by a teacher.

10. Printing from personal devices is not permitted at school.

11. Students are not to physically share their personal devices with other students, unless approved in writing by their parent/guardian.

12. Personal devices may not be used to cheat on assignments, tests or for non-instructional purposes, such as making personal phone call and text/instant messaging.

13. Personal devices may not be used to send inappropriate e-messages during the school day.

Standards of Responsible Use

All students in District schools must adhere to the following standards of responsible use:

- The District may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.
- Students are responsible at all times for their use of the District's electronic communication system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.
- Students must log in and use the District filtered wireless network during the school day on personal electronic devices.
- Students must not access, modify, download, or install computer programs, files, or information belonging to others.
- Students must not waste or abuse school resources through unauthorized system use (e.g. playing online games, downloading music, watching video broadcasts, participating in chat rooms, etc.).
- Students must not alter computers, networks, printers or other equipment except as directed by a staff member.
- Technology, including electronic communication, should be used for appropriate educational purposes only and should be consistent with the educational objectives of the District.
- Students must not release personal information on the Internet or electronic communications.
- If a student finds an inappropriate site or image, he or she must immediately minimize the program and contact the instructor.

- Students must not create/publish/submit or display any materials/media that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal and should report any instances encountered.
- Students shall adhere to all laws and statutes related to issues of copyright or plagiarism.
- Violation of any of these standards may result in suspension of computer use, Internet privileges and/or other disciplinary action.

Regulation approved: