THE SCHOOL DISTRICT OF TORRINGTON, CONNECTICUT

Student Use of Information Systems and Internet Safety

Policy

Computers, computer networks, electronic devices, Internet access, and e-mail are effective and important technological resources. The Board of Education provides computers, a computer network, including Internet access and an e-mail system, as well as other electronic devices that access the network such as wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing etc. (including, but not limited to, laptops, Kindles, radios, I-Pads or other tablet computers), referred to collectively as "the information systems," in order to enhance both the educational opportunities for our students and the business operations of the district.

These information systems are business and educational tools. As such, they are made available to students in the district for education related uses. Students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Additionally, the Board of Education will implement a technology protection measure to block or filter Internet access to visual depictions that contain obscene material, contain child pornography, or are harmful to minors and ensure that such filtering technology is operative during computer use by minor students.

As the owner of the information systems, the Board of Education reserves the right to monitor the use of the district's computers and information systems.

1. Information Systems

We are pleased to offer students access to the district's computers and computer networks, including access to electronic mail (e-mail) and the Internet, as well as electronic devices, (all of which will be referred to collectively as "information systems".) Access to the school's information systems will enable students to explore libraries, databases, and bulletin boards while exchanging messages with others. Such access is provided solely for education-related purposes. Use of the district's information systems will be allowed only for students who act in a considerate and responsible manner in using such systems.

The Board of Education and the Administration believe in the educational value of such information systems and recognize their potential to support our curriculum by expanding resources available for staff and student use. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

These information systems are expensive to purchase, install and maintain. As the property of the district these information systems must be

carefully handled and their integrity preserved for the benefit of all. Therefore, *access to the information systems is a privilege, and not a right.* Students will be required to adhere to a set of policies and procedures, as set forth in detail below. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board of Education's student discipline policy.

2. Definitions

Obscene – means any material or performance if, a) taken as a whole, it predominantly appeals to the prurient interest, b) it depicts or describes in a patently offensive way a prohibited sex act and c) taken as a whole, does not have serious literary, artistic, political or scientific value.

Child pornography –means any visual depiction, including any photograph, film, video, picture, cartoon, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where -

(a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
(b) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
(c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Harmful to minors – 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; and
(c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

3. Monitoring

Students are responsible for good behavior on school information systems just as they are in a classroom or a school hallway. Communications on the information systems are often public in nature and general school rules for behavior and communications apply. It is expected that users will comply with district standards and will act in a responsible and legal manner, at all times in accordance with district standards, as well as with state and federal laws.

It is important that students and parents understand that the district, *as the owner of the information systems, reserves the right to monitor and review* the use of these information systems. The district intends to monitor

and review in a limited fashion, but will do so as needed to ensure that the systems are being used for district-related educational purposes.

As part of the monitoring and reviewing process, the district will retain the capacity to bypass any individual password of a student or other user. *The system's security aspects, such as personal passwords and the message delete function for e-mail, can be bypassed for these purposes.* The district's ability to monitor and review is not restricted or neutralized by these devices. The monitoring and reviewing process also includes, but is not limited to; oversight of Internet site access, the right to review emails sent and received, the right to track students' access to blogs, electronic bulletin boards and chat rooms, and the right to review a student's document downloading and printing.

Therefore, all users must be aware that *they should not have any expectation of personal privacy in the use of these information systems.*

4. Student Conduct

Students are permitted to use the district's information systems for legitimate educational purposes. Personal use of district information systems is expressly prohibited. Conduct which constitutes inappropriate use includes, but is not limited to the following:

- Sending any form of harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);
- Gaining or seeking to gain unauthorized access to information systems;
- Damaging computers, computer files, information systems or computer networks;
- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from a teacher or administrator;
- Using another person's password under any circumstances;
- Trespassing in or tampering with any other person's folders, work or files;
- Sending any message that breaches the district's confidentiality requirements, or the confidentiality of students;
- Sending any copyrighted material over the system;
- Using information systems for any personal purpose, or in a manner that interferes with the district's educational programs;

- Accessing or attempting to access any material that is obscene, contains child pornography, or is harmful to minors, as defined above;
- Transmitting or receiving e-mail communications or accessing information on the Internet for non-educational purposes;
- Cyberbullying;
- Accessing or attempting to access social networking sites (e.g. Facebook, Twitter, MySpace, etc.) without a legitimate educational purpose.

In addition, as noted above, if a particular behavior or activity is generally prohibited by law, by Board of Education policy or by school rules or regulations, use of these information systems for the purpose of carrying out such behavior or activity is also prohibited.

Misuse of the information systems, or violations of these policies and regulations, may result in loss of access to such information systems as well as other disciplinary action, including suspension and/or expulsion, depending on the specific conduct.

Anyone who is aware of problems with, or misuse of these information systems, or has a question regarding the proper use of these information systems, should report this to his or her teacher or principal immediately. Most importantly, the Board of Education and the Administration urge *any* student who receives *any* harassing, threatening, intimidating or other improper message through the computer system to report this immediately. It is the Board of Education's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

5. Internet Safety

The Administration will take measures: to assure the safety and security of students when using e-mail, chat rooms, and other forms of direct electronic communications; to prohibit unauthorized access, including "hacking" and other unlawful activities by minors online; to prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; to educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response; and to restrict students' access to online materials harmful to minors, including obscene materials and child pornography.

6. Student Use Agreement

Before being allowed to use the district's information systems, students and/or their parents/guardians must sign a computer system use agreement, stating that they have read and understood the district's policies and regulations regarding the use of its information systems.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250 *et. seq.* (computer-related offenses)

Conn. Gen. Stat. § 53a-193 (definition of obscene)

18 U.S.C. § 2256 (definition of child pornography)

Electronic Communication Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. §§ 2510 through 2520

Children's Internet Protection Act, Pub. Law 106-554, codified at 47 U.S.C. § 254(h)

No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 U.S.C. § 6777

Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 U.S.C. § 254(h)(5)(B)(iii)

Miller v. California, 413 U.S. 15 (1973) (definition of obscene)