

Responsible Use For Students**I. Introduction**

Computers, computer networks, electronic devices, Internet access, and electronic mail are effective and important technological resources. The Board of Education provides computers, a computer network, including Internet access and an e-mail system, and may provide 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) to enhance the educational and business operations of the district. In this regulation, the computers, computer network, electronic devices, Internet access and electronic mail system are referred to collectively as "the computer systems."

These computer systems are business and educational tools. As such, they are being made available to students of the district for district-related educational and business purposes. The Board will 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. Additionally, the Board 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.

All users of the computer systems must restrict themselves to appropriate district-related educational and business purposes. Incidental personal use of the computer systems may be permitted solely for the purpose of e-mail transmissions and similar communications, including access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems is subject to all rules, including monitoring of all such use, set out in these regulations. Moreover, any such incidental personal use shall not interfere in any manner with school responsibilities.

These computer systems are expensive to install, own and maintain. As the property of the district these computer systems must be carefully handled and their integrity preserved for the benefit of all. Unfortunately, these computer systems can be misused in a variety of ways, some of which are innocent and others deliberate. In order to maximize the benefits of these technologies to the district and all our students, the regulations set forth below shall govern all use of these computer systems. Please be advised that access to the computer systems is a privilege, and not a right. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

II. Monitoring

It is important for all users of these computer systems to understand that the Board of Education, as the owner of the computer systems, reserves the right to monitor the use of the computer systems to ensure that they are being used in accordance with these regulations. The Board of Education intends to monitor in a limited fashion, but will do so as needed to ensure that the systems are being used appropriately for district-related educational purposes and to maximize utilization of the systems for such educational purposes.

Responsible Use For Students

II. Monitoring (continued)

Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, Instagram, YouTube, and Snapchat.

III. Why Monitor

The computer systems are expensive for the Board to install, operate and maintain. For that reason alone it is necessary to prevent misuse of the computer systems. However, there are other equally important reasons why the Board intends to monitor the use of these computer systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees.

These computer systems can be used for improper, and even illegal, purposes. Experience by other operators of such computer systems has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of others, threatening others, breaches of confidentiality, copyright infringement and the like.

Monitoring will also allow the Board to continually reassess the utility of the computer systems, and whenever appropriate, make such changes to the computer systems as it deems fit. Thus, the Board monitoring should serve to increase the value of the system to the district on an ongoing basis.

IV. Privacy Issues

The Board reserves the right to conduct monitoring of these computer systems and can do so despite the assignment to individual students of passwords for system security. Any password systems implemented by the district are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user.

The system's security aspects, message delete function and personal passwords can be bypassed for monitoring purposes.

Therefore, students must be aware that they should not have any expectation of personal privacy in the use of these computer systems. This provision applies to any and all uses of the district's computer systems and electronic devices that access same, including any incidental personal use permitted in accordance with these regulations.

Use of the computer system represents an employee's acknowledgement that the student has read and understands these regulations and any applicable policy in their entirety, including the provisions regarding monitoring and review of computer activity.

INSTRUCTION

6141.321a

Responsible Use For Students

V. Prohibited Uses

Inappropriate use of district computer systems is expressly prohibited, including, but not limited to, the following:

1. Sending any form of solicitation not directly related to the business of the Board of Education or approved by the Superintendent;
2. Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);
3. Gaining or seeking to gain unauthorized access to computer systems;
4. 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;
5. Sending any message that breaches the Board of Education's confidentiality requirements, including the confidentiality rights of students;
6. Sending any copyrighted material over the system;
7. Sending messages for any purpose prohibited by law;
8. Transmission or receipt of inappropriate e-mail communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;
9. Using computer systems for any personal purposes, or in any manner, other than those permitted under these regulations, that interferes with the district's educational programs;
10. Accessing or attempting to access any material that is obscene, contains child pornography, or is harmful to minors, as defined below;
11. Using social networking sites such as Facebook, Twitter, Instagram and Snapchat in a manner that (i) interferes with the work of the school district without a legitimate educational purpose; (ii) harasses or cyberbullies other students, school personnel, or other members of the school community; (iii) breaches the district's confidentiality requirements, or the confidentiality of students; (iv) disrupts the work of the school district; (v) harms the goodwill and reputation of the school district in the community or (vi) otherwise violates the law, Board of Education policies and/or other school rules and regulations.

INSTRUCTION

6141.321a

Responsible Use For Students

VI. 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.

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. For the purposes of this section, "prohibited sex act" means erotic fondling, nude performance, sexual excitement, sado-masochistic abuse, masturbation or sexual intercourse.

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.

Responsible Use For Students

VII. Electronic Communications

The Board expects that all students will conform with all applicable Board policies and standards of professional conduct when engaging in any form of electronic communication, including texting, using the district's computer system, or through the use of any electronic device or mobile device owned, leased, or used by the Board. The Board recommends students exercise caution and appropriate judgment when using electronic communications with other students, teachers, administrators and other individuals in the context of fulfilling a student's school-related responsibilities.

VIII. Disciplinary Action

Misuse of these computer systems will not be tolerated and may result in loss of access to computer systems as well as disciplinary action, up to and including, suspension and/or expulsion, depending on the specific conduct. The Superintendent reserves the right to eliminate use of the district's computer systems by any or all students at any time.

IX. Complaints of Problems or Misuse

Anyone who is aware of problems with, or misuse of these computer systems, or has a question regarding the appropriate use of the computer systems, should report this to his or her teacher or administrator immediately.

Most importantly, the Board urges any student who receives any harassing, threatening, intimidating or other improper message through the computer systems to report this immediately. It is the Board'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!

X. Implementation

Students will receive a copy of this policy and be required to acknowledge that they have read and understand the policy.

Legal References: Children's Internet Protection Act, Pub. Law 106-554, codified at 47 U.S.C. § 254(h)
Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520
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)
18 U.S.C. § 2256 (definition of child pornography)
Miller v. California, 413 U.S. 15 (1973) (definition of obscene)
Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250 (computer-related offenses)
Conn. Gen. Stat. § 53a-193 (definition of obscene)

Regulation Revised: 02/25/13, 06/18/18

