

ADMINISTRATIVE REGULATIONS REGARDING STUDENT USE OF THE DISTRICT'S COMPUTER SYSTEMS AND INTERNET SAFETY

1. Introduction

a. *Access to District Computer Systems When Students Are Physically Present on School Property*

When students are physically present on Torrington Public Schools (“District”) property, the Torrington Board of Education (the “Board”) is pleased to offer students access to the District's computers and computer networks, including access to electronic messaging systems (including email) and the Internet, as well as electronic devices (all of which will be referred to collectively as "computer systems"). Access to the school's computer systems will enable students to explore online resources, including but not limited to libraries, blogs, wikis, databases, websites, and bulletin boards, while exchanging information with others. Such access is provided solely for education-related purposes. Use of the District's computer systems will be allowed only for students who act in a considerate and responsible manner in using such systems.

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

These computer systems are expensive to purchase, install and maintain. As the property of the District, these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students are required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board’s student discipline policy.

b. *Access to District Computer Systems When Students Are Engaged in Digital or Remote Learning*

The Board and the Administration recognize that technology is integral to the delivery of instruction if and when the District implements any form of digital or remote learning. The District may therefore provide students with remote access to some or all of the District’s computer systems so that students may access the District’s virtual learning environment. Such access, if granted, is provided solely for education-related purposes. Use of the District's computer systems will be allowed only for students who comply with District policies and procedures concerning computer system use, and demonstrate the ability to use the computer systems in a considerate and responsible manner.

These computer systems are expensive to purchase, install and maintain. As the property of the District, these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, students will be required to adhere to a set of policies and procedures, as set forth in detail below, in conjunction with their use of the computer systems. Violations may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board'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 sexual act and c) taken as a whole, it lacks serious literary, artistic, educational, political or scientific value.

"Obscene as to minors" means any material or performance if it depicts a prohibited sexual act and, taken as a whole, it is harmful to minors.

For purposes of this section, **"harmful to minors"** means that quality of any description or representation, in whatever form, of a prohibited sexual act, when a) it predominantly appeals to the prurient, shameful or morbid interest of minors, b) it is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors, and c) taken as a whole, it lacks serious literary, artistic, educational, political or scientific value for minors.

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

“Child sexual abuse material” includes child pornography and means any visual depiction, including any photograph, film, video, picture, 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 a digital image, computer mage, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

3. Monitoring

Students are responsible for good behavior on school computer systems just as they are in a classroom or a school hallway. Communications on the computer systems are often public in nature and general school rules for behavior and communications apply. It is expected that students 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 computer systems, reserves the right to monitor and review* the use of these computer 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 email, 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 electronic messages sent and received, the right to track students' access to blogs, electronic bulletin boards and online communication platforms, and the right to review a student's data downloading and printing.

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

4. Student Conduct

Students are permitted to use the District's computer systems for legitimate educational purposes. Personal use must be specifically authorized by a District staff member. Unauthorized personal use of District computer systems is expressly

prohibited. Conduct which constitutes inappropriate use includes, but is not limited to the following:

- ◆ Sending any form of a harassing, threatening, or intimidating message, at any time, to the extent such communication may violate other applicable Board policy, regulation, or school rule (such communications may also be a crime);
- ◆ Gaining or seeking to gain unauthorized access to computer systems;
- ◆ Damaging computers, computer files, computer 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 responsible school staff member;
- ◆ 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 other students;
- ◆ Sending any copyrighted material over the systems;
- ◆ Using computer 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, obscene as to minors, or contains child sexual abuse material, as defined above;
- ◆ Transmitting or receiving electronic communications or accessing information on the Internet for non-educational purposes;
- ◆ Cyberbullying;
- ◆ Accessing or attempting to access social networking sites (e.g., Facebook, Twitter/X, Instagram, Snapchat, TikTok, YouTube etc.) without a staff member's authorization and/or a legitimate educational purpose;
- ◆ The unauthorized use of generative artificial intelligence on any of the Board's computer systems. For purposes of this policy, "generative

artificial intelligence” refers to a technology system, including but not limited to ChatGPT, capable of learning patterns and relationships from data, enabling it to create content, including but not limited to text, images, audio, or video, when prompted by a user.

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

Misuse of the computer systems, or violations of these policies and regulations, may result in loss of access to such computer 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 computer systems, or has a question regarding the proper use of these computer systems, should report or discuss the issue with a teacher or the school principal immediately. Most importantly, the Board 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'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 digital safety and security of students when using electronic messaging systems, email, chat rooms, distance learning platforms, 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 cyberbullying awareness and response; and to restrict students’ access to online materials that are obscene or obscene as to minors or contain child sexual abuse material, to the extent practicable when students are using Board-owned computers or devices and Board-provided Internet access.

6. Student Use Agreement

Before being allowed to use the District’s computer 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 computer systems.

Legal References:

Conn. Gen. Stat. § 10-221

Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-193; 53a-250 *et. seq.* (computer-related offenses)

Conn. Gen. Stat. § 53a-193 (definition of obscene and obscene as to minors)

Public Act 24-118, “An Act Concerning Child Sexual Abuse.”

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

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 through 2523

Children’s Internet Protection Act, 47 U.S.C. § 254(h)

No Child Left Behind Act of 2001, 20 U.S.C. § 6777

Protecting Children in the 21st Century Act, 47 U.S.C. § 254(h)(5)(B)(iii)

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