Students

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 school property, the Board is 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 "computer systems"). Access to the school's computer systems will enable students to explore libraries, databases, websites, and bulletin boards (e.g. blogs, discussion boards, digital classroom, etc.) 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 of Education and the Administration believe in the educational value of such computer 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 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 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 pornography – means any visual depiction, including any photograph, film, video, picture, 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 image 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 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 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 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 computer systems.*

4. Student Conduct

Students are permitted to use the district's computer systems for legitimate educational purposes. 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 any person (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 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 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 pornography, , 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, Instagram, Snapchat, TikTok, etc.) without a legitimate educational purpose.

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 this to his or her teacher or 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 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 cyber-bullying awareness and response; and to restrict students' access to online materials that are obscene or obscene as to minors or contain child pornography, 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.

Code of Conduct Guidelines for District Users

The purpose of providing Internet and other computer network access in this district is to promote the exchange of information and ideas with the global community. The following represents a guide to the acceptable use of the technology provided by this district. All network use must be consistent with the policies and goals of this school district. Inappropriate use of district technology will result in the loss of technology use, disciplinary action, and/or referral to legal authorities.

All Internet and other computer network users will be expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. The use of technology in the district shall not be used to harass others.

2. Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online[1].

3. Protect password confidentiality and respect the privacy of others.

4. Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birth dates, and pictures. Do not share your password with the exception of teachers and parents.

5. It is necessary to be mindful of and adhere to laws and regulations relative to copyright infringement, plagiarism, and illegal activities and downloading.

6. The district technology is not to be used for playing non-educational/non-approved multi-user or other network intensive games.

7. No charges for services, products, or information are to be incurred without appropriate permission.

8. Be aware that electronic mail, social media, and network storage/use are not guaranteed to be private. Administration has the right to monitor all student and employee use of district computers and other district electronic devices. Students and employees should have no expectation of personal privacy in any communication while using district technology. Messages relating to or in support of illegal activities may be reported to the proper authorities. The district expects professional etiquette from all users engaged in social media.

9. Do not use the network in such a way that you would disrupt the use of the network by their users (for example, ongoing live video stream).

10. Vandalism, theft, or malicious actions will not be tolerated.

11. Report security problems to the supervising teacher or system administrator.

12. Users will not open or attempt to repair any computer hardware without the prior approval of Instructional Technology (IT) personnel.

13. Users will not install or attempt to install hardware or software on any computer.

14. Users will not connect, attempt to connect or disconnect any computer or peripheral (eg. Printers) to or from the network without the prior approval of Instructional Technology (IT) personnel.

15. Users are not permitted and should never attempt to modify the operating system of the device.

16. Users must report any inappropriate site to proper authorities and should leave an inappropriate site immediately when accessing such a site in error.

17. Users will not employ the network for commercial or personal business purposes such as selling or purchasing personal items or solicitation of non-district related fundraisers or activities.

18. If users have a district digital device for school use, all confidential files need to be saved using encryption software. Whenever possible, confidential files should be saved to the appropriate network drive.

19. Unless authorized by a certified staff member, users will not visit a personal blog during instructional periods.

20. All users should adhere to the social media policy.

21. Unless otherwise notified, the district will assume permission is given to publish students' name, work, video and photographs.

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 and obscene as to minors)

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)

Regulation approved:	October 4, 2004	STAFFORD PUBLIC SCHOOLS
Regulation reviewed:	August 18, 2008	Stafford Springs, Connecticut
Regulation revised:	August 20, 2012	
Regulation revised:	January 30, 2017	
Regulation revised:	August 23, 2021	