

**5135  
Students**

**POLICY REGARDING STUDENT USE OF  
THE DISTRICT'S COMPUTER SYSTEMS AND INTERNET SAFETY**

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, Internet access, an e-mail system, as well as other electronic devices that access the network such as wireless and/or portable 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, personal laptops, Smartphones, network access devices, cellular telephones, radios, MP3 and other digital audio players, CD players tablet computers, walkie-talkies, personal data assistants, digital cameras, and other electronic signaling devices (referred to collectively as "Computer Systems")), in order to enhance both the educational opportunities for our students and the business operations of the District.

These Computer Systems are business and educational tools. As such, they are made available to students in the District for education related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such Computer Systems are used by students solely for education related purposes. The Board will educate 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 sites that contain obscene material, contain child pornography, or are harmful to minors and ensure, to the extent possible, that such filtering technology is operative during computer use by students.

As the owner of the Computer Systems, the Board reserves the right to monitor the use of the Computer Systems.

**Legal References:**

- Children's Internet Protection Act, Pub. L. 106-554, codified at 47 U.S.C. § 254(h)
- Conn. Gen. Stat. §§ 53a-182b; 53a-183; 53a-250
- 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)

**Policy References:**

**Policy No. 5114, Student Discipline**

**Policy No. 5131.911, Bullying**

**Regulation No. 5131.911, Safe School Climate Plan**

**Policy 5136, Use of Privately Owned Technological Devices By Students**

**Policy No. 6184, Unexpected Broadcast**

**ADOPTED: August 20, 2001**

**REVISED: August 20, 2007**

**June 17, 2013**

**WESTON PUBLIC SCHOOLS**  
**Weston, Connecticut**

**R5135  
Students**

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

Introduction

Weston Public Schools ("the District") is pleased to offer students access to the Board's computers and computer networks, including access to electronic mail (e-mail) and the Internet, as well as electronic devices described in Policy Number 5135, (all of which will be referred to collectively as "Computer Systems".) Access to the Computer 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 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 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, *access to the Computer 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's student discipline policy.

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 sex act and c) taken as a whole, does not have serious literary, artistic, political or scientific value. For the purposes of this section, "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; or
- (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, other visual depiction, or audio recording 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.

### Monitoring

Students are responsible for good behavior on the 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 Board, as the owner or lessee 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 it deems appropriate to ensure that the Computer 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 electronic communications sent and received the right to track students' access to blogs, electronic bulletin boards, social media, 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.*

## Student Conduct

Students are permitted to use the District's Computer Systems for legitimate educational purposes. Personal use of District Computer Systems by elementary school and intermediate school students is expressly prohibited. Personal use of the Computer Systems by high school and middle school students is permitted. Such personal use of the Computer Systems by middle and high school students, however, is subject to all Board policies and regulations, including monitoring of all such use, as well as any rules that the Superintendent may establish. Moreover, any such personal use shall not interfere in any manner with instructional time, and under no circumstances should such personal use occur during class.

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 other "computer systems" as that term is defined above;
- Using another person's password and/or username to access that person's account or otherwise attempt to gain unauthorized access to the Computer Systems;
- Misrepresenting oneself as another individual or entity and/or modifying files, communications, other data, passwords or usernames belonging to another person and/or to which access is not otherwise available to the student;
- 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;
- Trespassing in or tampering with any other person's folders, work, communications, files, or other data;
- Sending any message that breaches the District's confidentiality requirements, or the confidentiality of students;
- Failing to adhere to copyright laws including, but not limited to, using the Computer Systems to reproduce, copy, save, improperly cite,

and/or distribute materials subject to copyright except as permitted by law;

- Using the Computer Systems for any personal purpose, except as provided in these Regulations, 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 as defined in Policy and Administrative Regulation 5131.911;

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. Further, if the conduct may constitute criminal activity, law enforcement may be notified.*

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 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* to the school.

### Internet Safety

The Administration will take measures, as it deems appropriate: to assure the safety and security of students when using District managed e-mail, chat rooms, social media, and other forms of direct electronic communications; to prohibit unauthorized access of the Computer Systems, including "hacking" and other unlawful activities online; to prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students available on the Computer Systems; to educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying (as defined in Policy and

Regulation No. 5131.911) awareness and response; and to restrict students' access to online materials harmful to minors, including obscene materials and child pornography.

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)

Policy References:

Policy No. 5114, Student Discipline  
Policy No. 5131.911, Bullying  
Regulation No. 5131.911, Safe School Climate Plan  
Policy 5136, Use of Privately Owned Technological Devices By Students  
Policy No. 6184, Unexpected Broadcast

ADOPTED: August 20, 2007  
REVISED: June 17, 2013

WESTON PUBLIC SCHOOLS  
Weston, Connecticut