

STUDENTS

Technology Acceptable Use Policy

Computers, computer networks, internet access, and e-mail are effective and important technological resources in today's educational environment. The Board of Education has installed computers, a computer network, including Internet access and an e-mail system (referred to collectively as "the computer systems"), in order to enhance both the educational opportunities for our students and the business operations of the District.

As the owner of the computer systems, the Board reserves the right to monitor the use of the District's computers and computer systems. When personal devices are used on the District network, they are considered part of the computer system and therefore are subject to monitoring by the District and the subject of this and other related policies. These computer systems are business and educational tools. As such, they are made available to students in the District for educational 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 educational purposes. The Board will educate students about appropriate online behavior, including cyberbullying, and interacting with other individuals on social networking websites and-in chat rooms. Additionally, the Board will implement technology protection measures to block or filter internet access to visual depictions that contain obscene material, contain child pornography, or are harmful to minors. The administration will ensure that such filtering technology is operative at all times.

Students are allowed to use privately owned technology devices for educational purposes at the discretion of the faculty and in accordance with appropriate use guidelines to be determined by the principal or principal's designee. Privately owned technology devices will be permitted access to the school network only through Board-provided network accounts, and all such access will be monitored and filtered by the District's technology protection measures. All use of privately owned technology devices is subject to this Technology Acceptable Use policy, the Discipline Policy (5114) and the Regional School District 13 Core Ethical Values. Violations may result in revocation of access to and privileges relating to use of the computer systems, and to disciplinary action, up to and including suspension and/or expulsion.

Responsibilities

Building principals are responsible for ensuring that use of the computer systems by students is supervised by faculty in accordance with school and District policies and monitored by the technical staff as needed. Building principals shall also determine which privately owned technology devices will be permitted in their school and establish guidelines for their use.

The Superintendent of Schools or his/her designee will be responsible for implementing this policy, establishing procedures and guidelines and supervising access privileges. Such guidelines shall be used to enforce the measures to block or filter internet access and to preserve the rights of both students and staffs to examine and use information to meet the educational goals and objectives of Regional District 13.

Classroom teachers are responsible for employing technology in relevant ways to meet the District's Technology Integration Standards and Benchmarks, providing training to students as needed, and supervising student use of computer systems as directed by the principal in accordance with school and District policies.

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 Adopted: February 11, 2009
Policy Reviewed: February 8, 2011
Policy Revised: October 12, 2011
Policy Revised: May 23, 2012

STUDENTS - Regulation

Computer Use and Internet Safety

Introduction

The District offers students access to the District's computers and computer networks, including access to electronic mail (e-mail) and the internet (that will be referred to collectively as "computer systems". This also includes privately owned technology devices.) Access to the school's computer systems will enable students to explore libraries, databases, and bulletin boards while exchanging messages with others. Such access is provided solely for educational purposes. Use of the District's computer systems will be allowed exclusively for students who comply with all District policies and procedures pertaining to the District's computer systems.

Access to the computer systems or computer network, and use of privately owned technology devices on the school network is a privilege, and not a right. Violations to this policy may lead to withdrawal of the access privilege and/or disciplinary measures in accordance with the Board's student discipline policy.

Monitoring

It is important that students and parents understand that the District, as the owner of the computer systems, will monitor the use of these computer systems at all times even if they are accessed from privately owned technology devices.

As part of the monitoring and reviewing process, the District will retain the authority 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 may 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 student access to blogs, electronic bulletin boards and chat rooms, and the right to review student document downloading and printing.

All users must be aware that they shall not have any expectation of personal privacy in the use of District computer systems.

Student Conduct

Students are permitted to use District computer systems exclusively for legitimate educational purposes. Personal use of the District computer systems is expressly prohibited. Conduct that constitutes inappropriate use includes, but is not limited to the following:

1. Cyberbullying or any other form of harassing, threatening, or intimidating message, at any time, to any person (such communications may also be a crime);
2. Gaining or seeking to gain unauthorized access to computer systems;
3. Damaging computers, computer files, computer systems or computer networks;
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. Using another person's password under any circumstances;
6. Trespassing in or tampering with any other person's folders, work or files;
7. Sending any message that breaches the District's confidentiality requirements, or the confidentiality of students;
8. Sending unauthorized copyrighted material over the system;
9. Using computer systems for any personal purpose, or in a manner 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;
11. Transmitting or receiving e-mail communications or accessing information on the Internet for non-educational purposes.

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, or legal action if the misuse is constituted a criminal activity. Further, the District will cooperate with law enforcement.

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.

Internet Safety

The Administration will take measures: to ensure 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 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 harmful to minors, including obscene materials and child pornography.

Privately Owned Technology Devices

Students are permitted to use privately owned technology devices in school and to access the school network during the school day for educational purposes. Use of privately owned technology devices by students is allowed under the following conditions:

1. When they focus on the educational uses of personal technology and their appropriate use and etiquette in a public setting.
2. When the use is at the discretion of the teacher. Students will be able to use devices only in the manner that each teacher permits, and are not to use them in class at other times or for other uses.
3. When they are used in non-classroom settings, they will be permitted as long as they do not interfere with education, the learning environment, or the functioning of the classroom or school.

Guidelines for using privately owned devices are:

- A. Devices are permitted in the cafeteria and library during unstructured times and in study halls. Earphones must be used, and only at a volume that allows a person speaking to be heard easily.
- B. Earphones will not be permitted in hallways.

Privately owned devices are the responsibility of the students who bring them to school, and no student will be required to bring their devices to school. The school will not assume any responsibility for devices that are lost or damaged in any way if students choose to bring them to school.

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 Adopted: February 11, 2009
Regulation Reviewed: February 8, 2011
Regulation Revised: October 12, 2011
Regulation Revised: May 23, 2012