Series 6000: Instruction

Internet and Computers

Acceptable Use and Internet Safety

The Board of Education provides computers, a computer network, including Internet access and an email system, as well as electronic devices such as cellular telephones and personal data assistants (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.

The Board believes the educational opportunities inherent in these tools far outweigh the possibility that users may procure material not consistent with the education goals of Southington Public Schools. However, the Internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to students. The Board acknowledges that while it is impossible to predict with certainty what information students might locate or come into contact with, it shall take all reasonable steps to protect students from accessing material and information that is obscene, pornographic or otherwise harmful to minors.

The Board shall 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. Additionally, students shall take responsibility for their own use of school computers and computer systems to avoid contact with material or information that may be harmful.

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 minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

As the owner of the computer systems, the Board reserves the right to monitor the use of the district's computers and computer systems.

Series 6000: Instruction

Internet and Computers

Acceptable Use and Internet Safety

Legal References:
Children's Internet Protection Act, Pub. L. 106-554, codified at 47 USC §254h
CT General Statute: §§53a-182b; 53a-183; 53a-250
Electronic Communication Privacy Act, 18 USC §§2510-2520
No Child Left Behind Act of 2001, Pub. L. 107-110, codified at 20 USC §6777
Protecting Children in the 21st Century Act, Pub. Law 110-385, codified at 47 USC §254(h)(5)(B)(iii)

Policy Adopted: February 2009
Policy Revised: May 2011
Policy Revised: June 2011

Series 6000: Instruction

Internet and Computers

Acceptable Use and Internet Safety Procedures

We are pleased to offer students access to the district's computers and computer networks, including access to electronic mail (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 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.

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. 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 in accordance with the Board's student discipline policy.

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 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 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.

Series 6000: Instruction

Internet and Computers

Acceptable Use and Internet Safety Procedures (continued)

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

Blocking or Filtering Obscene, Pornographic, and Harmful Information
Software blocks or filters material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the Board, from reaching all school computers having Internet or electronic communications access. Students shall report access to material and information that is obscene, pornographic, harmful to minors or otherwise in violation of this policy to the supervising staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.

No Expectation of Privacy
School computers and computer systems are owned by Southington Public Schools and are intended for educational purposes at all times. Students shall have no expectation of privacy when using the Internet or electronic communications. The administration reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district computers and computer systems, including all Internet and electronic communications access and transmission or receipt of materials and information. All material and information accessed or received through district computers and computer systems shall remain the property of Southington Public Schools.

Unauthorized and Unacceptable Users
Students are permitted to use the district's computer systems for legitimate educational purposes. Personal use of district computer systems is expressly prohibited.

Because technology and ways of using technology are constantly evolving, every unacceptable use of school computers and computer systems cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

No student shall intentionally access, create, transmit, retransmit or forward material or information that:

Series 6000: Instruction

Internet and Computers

Acceptable Use and Internet Safety Procedures (continued)

- Is not related to Southington Public Schools education objectives;
- Promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons;
- Contains pornographic, obscene or other sexually oriented materials, either as pictures or writings;
- Harasses, threatens, demeans or promotes violence or hatred against another person or group of persons with regard to race, color, sex, religion, national origin, age, marital status, disability or handicap;
- Is for personal profit, financial gain, advertising, commercial transaction or political purposes;
- Plagiarizes the work of another;
- Uses inappropriate or profane language offensive in the school community;
- Is knowingly false or could be construed as intending to purposely damage another person's reputation;
- Is in violation of any federal or state law, including but not limited to copyrighted material and material protected by trade secret;
- Contains personal information about themselves or others, including information protected by confidentiality laws;
- Uses another individual's Internet or electronic communications account;
- Impersonates another or transmits through an anonymous remailer;
- Accesses fee services without specific permission from the system administrator;
- Constitutes cyberbullying; and
- Accesses or attempts to access social networking sites (e.g. Facebook, Twitter, MySpace, etc.) without a legitimate educational purpose.

Security

Security on the district computer systems is a high priority. Students who identify a security problem while using the Internet or electronic communications must immediately notify an administrator. Students shall not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use another person's password or any other identifier;
- gain or attempt to gain unauthorized access to district computers or computer systems; and
- trespassing in or tampering with any other person’s folders, work or files.

Series 6000: Instruction

Internet and Computers

Any user identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications.

Safety

The administration will take measures: to assure the safety and security of students when using email, 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 cyberbullying awareness and response; and to restrict students' access to online materials harmful to minors, including obscene materials and child pornography.

Vandalism

Vandalism will result in cancellation of privileges and may result in school disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt operation of any network within the district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized Software

Students are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner.

Series 6000: Instruction

Internet and Computers

Assigning Student Projects and Monitoring Student Use

Southington Public Schools will make every effort to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers, and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

All students shall be supervised by staff while using the Internet or electronic communications.

Student Use is a Privilege

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the Internet and electronic communications is a privilege, not a right. Failure to follow the procedures contained in this policy will result in the loss of the privilege to use these tools and may result in school disciplinary action and/or legal action. Administration may deny, revoke or suspend access to district technology or close user accounts at any time.

No Warranties

The district makes no warranties of any kind, whether expressed or implied, related to the use of school computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement of the content, nor make any guarantee as to the accuracy or quality of information received. The district shall not be responsible for any damages, losses or costs a student suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the students' own risk.

Series 6000: Instruction

Internet and Computers (continued)

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 2009
Regulation Revised: May 2011