Series 6000 - Instruction

I. Elementary and Secondary

D. Curriculum

(1) Curriculum Design/Development/Revision

(c) Computer Literacy

(i) Computers: ~~Acceptable~~ Responsible Use of the Internet, Other Computer Networks and Internet Safety

The Suffield Public Schools provides computers, networks and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff.

Employees should be aware that the Suffield Public Schools may monitor usage of electronic resources by individuals and that all electronic resources have been provided to employees of Suffield Public Schools to support the business and educational purposes. Employees and staff of the Suffield Public Schools are responsible for ensuring that they understand and follow this policy. Students promise to only use technology and digital resources in support of learning activities. Students must ensure that they legally:

- Use real-world digital and other research tools to access, evaluate and effectively apply information appropriate for authentic tasks;
- Work independently and collaboratively to solve problems and accomplish goals;
- Communicate information clearly and effectively using a variety of tools/media in varied contexts for a variety of purposes;
- Demonstrate innovation, flexibility, and adaptability in thinking patterns, work habits, and working/learning conditions;
- Effectively apply the analysis, synthesis, and evaluative processes that enable productive problem solving; and
- Value and demonstrate personal responsibility, character, cultural understanding, and ethical behavior.

Policy adopted: August 20, 2002
Policy revised: July 8, 2008, August 21, 2012

SUFFIELD PUBLIC SCHOOLS
Suffield, Connecticut

Series 6000 - Instruction

I. Elementary and Secondary

D. Curriculum

(1) Curriculum Design/Development/Revision

(c) Computer Literacy

(i) Computers: ~~Acceptable~~ Responsible Use of the Internet, Other Computer Networks and Internet Safety

Suffield Public Schools (the "District") is pleased to offer students access to District computers and instructional technologies, communications and data management systems, informational technologies and the Internet, and an array of other technology resources to promote educational excellence and innovation. While using District provided and personal technology resources on school property, in school vehicles and buses, at school-sponsored activities, or using District technology resources via off-campus remote access, each student must act in an appropriate, ethical manner consistent with school, District, and legal guidelines. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about his/her responsibilities, to establish expectations, and to monitor student behavior when using technology.

Access to District technology resources is provided to students who act in appropriate and responsible ways. Prior to being allowed access to the Internet at school or through technology resources provided through the District, students and their parents must sign the District's Responsible Use Agreement acknowledging their responsibilities. Students must comply with all District regulations and protocols to be permitted the use of District technology resources.

The District's technology resources are provided to students to conduct research, access curriculum resources, enhance parent and student involvement in the educational process, complete assignments, and communicate effectively. The District grants access to its District technology resources as a privilege for students who conform to behavioral expectations with respect to use of technological resources. Just as students are responsible for making good behavior decisions in a classroom or on school grounds, they are responsible for making good decisions when using District technology resources or personal technology in a manner that impacts the school environment.

If a student violates any of these rules, his/her use of the District's technology resources may be terminated and future access may be denied. A violation may also result in a prohibition on the use and/or possession of personal technology on school property. Formal disciplinary action may also result. If possible criminal activity is discovered, the proper law enforcement authorities may be notified. Disciplinary action for students shall be in accordance with existing discipline policies and may include suspension or expulsion.

Definitions

District Technology Resources:

For the purposes of the District's BYOT policy, "District Technology Resources" refers to District's computers, District issued personal devices (including Smartphones and other mobile or handheld devices) and instructional technologies; communications and data management systems; informational technologies and the Internet; and a variety of other technology resources in order to promote educational excellence.

Personal Technology:

For the purposes of the District's BYOT policy, "personal technology" refers to privately owned wireless and/or portable ~~electronic 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. These devices may include, but are not limited to, personal laptops, net books, Smartphones, network access devices, and other electronic signaling devices.

Applicable Standards for Use of District Provided Technology Resources

In addition to the general principles set forth in this Student Responsible Use Policy, the use of District technology resources may be affected by a number of other legal and ethical principles. While it is not possible to list all potentially applicable laws, regulations, and local standards, the following are provided:

The District technology resources shall only be used to access educational information and to promote learning activities both at school and home, including the facilitation of communications between the home and school.

Students shall not load personal software or programs on District computers, nor shall they download programs from the Internet without the approval of their instructor.

Virtual and physical vandalism shall not be tolerated. Any intentional act by a student that damages or interferes with performance of District technology hardware, software, opersystems, or communication and data management systems will be considered vandalism and will be subject to school discipline and/or appropriate criminal or civil action.

Not all access to the Internet can be supervised. Students agree not to send, access, submit, publish, display, or print over the Internet or the District network, or using the District technology resources, any defamatory, abusive, obscene, profane, sexually- oriented, threatening, offensive, or illegal material. The use of District technology resources in a manner intended to injure or humiliate others by disclosure of personal information (whether true or false), by personal attacks on others, by disparaging statements, expressed toward any person, or by disparagement of any person's or group's race, color, religion, national origin, gender, sexual orientation, or disability are strictly prohibited. Cyberbullying, as defined in Board policy 5131.913, is also specifically prohibited. It shall be the student's responsibility to immediately report any inappropriate use to the student's teacher or another staff member.

Although the District uses software filters to block known inappropriate web sites and prohibit access to harmful materials accessed from a District network, the District does not filter or block access to harmful materials accessed from District-provided technology resources that are being used outside of the District network. Even in the best of circumstances, filtering technology is not perfect and therefore may, in effect, both interfere with legitimate educational purposes and allow some objectionable material to be viewed.The use of the District technology resources is not private. Students should not expect that files stored on or transmitted via the District's resources will be confidential. All digital transmissions are subject to monitoring by District employees and other officials. Digital storage is the District's property, and as such, district technology staff may review files and communications to maintain system integrity and ensure that students are using technology responsibly.The District denies any responsibility for the accuracy of information obtained from the Internet or on-line resourThe District makes no warranties of any kind, expressed or implied, for the technology resources it provides to students.Copyright ©, Trademark ™ and/or Registered ® laws must be adhered to at all times. All materials from the Internet and other digital resources, including graphics, which are used in student projects or reports, must be properly cited. Copyrighted, Trademarked or Registered materials may not be placed on the Internet without the permission of the author.

Students shall not post or transmit their own or other's personal information such as home addresses, telephone numbers, or other personal identifying information. Last names and photos shall never be posted without the permission of all identifiable subjects.

The use of District technology resources involves the use of a password, network access code, or other identifying or validating code. Such passwords and codes are to be protected as private information provided to the individual user for their sole use and purpose.

Such passwords and codes shall not be disclosed by student to others. Students are specifically prohibited from gaining or seeking to gain unauthorized access to District technology resources, from using another person's password under any circumstances, and from trespassing in or tampering with any other person's folders, work or files.

Students shall not use District technology resources to conduct business activities or use District technology resources for any personal purpose, or in a manner that interferes with the District's educational programs. Students shall not use District technology resources for advertising, promotional or commercial purposes or similar objectives, including the purchase of any items or services.

Students may bring personal technology, including computers, Smartphones, network access devices, net books, other personal computers or other electronic signaling devices to school provided that such technology is used for instructional purposes. Students shall abide by the instructions provided by teachers and other school staff in the use of such personal technologies. Access to the Internet or other District technology resources from personal technology is limited to wireless access points on the school campuses or other access devices away from school. Access to the Internet or other District technology resources from personal technology is not available via hardwired connections.

Network Access by Students Using Personal Technology

Students accessing the District's wireless network must abide by the protocols outlined in the District's "Bring Your Own Technology (BYOT)" policy and the following administrative regulations:

Students are fully responsible for all of the personal technology they bring to school.

Students will access the District's wireless network using their school account log-ins and passwords. Students are advised that the District's network administrators have the capability to identify users and to monitor all BYOT devices while they are logged on to the network. 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 District technology 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 the following: 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.

Students and parents should be aware that the District is not liable for any student's personal technology that is lost, stolen, or damaged.

No personal technology can be used during any assessments or tests, unless otherwise directed by the teacher.

Students must immediately comply with teachers' requests to shut down personal technology devices or close their screens. Personal technology devices must be in silent mode when not in use, and put away when directed by a teacher or other school staff member.

Students are not permitted to transmit or post photographic images or videos on public and/or social-networking sites which they have taken of any person on school grounds.

Personal technology devices must be charged prior to bringing them to school and must operate using their own batteries while at school.

To ensure appropriate network filtering, students will only use the BYOT wireless connection in school and will not attempt to bypass the network restrictions by using 3G or 4G networks.

Students will be held accountable for knowingly infecting the District's technology resources with a virus, malware, or any program designed to damage, alter, destroy, or provide access to unauthorized data or information. These actions are a violation of the Student Responsible Use Policy and will result in disciplinary consequences and criminal prosecution, if applicable. The District has the right to collect and examine any personal technology device that is suspected of causing problems or is the source of an attack or virus infection.

Students may only access electronic files or Internet sites which are relevant to the classroom curriculum and/or suggested by a teacher or other staff member for educational purposes. Students are prohibited from processing or accessing information related to "hacking," altering, or bypassing network security policies, and they will be subject to disciplinary consequences and criminal prosecution, if applicable.

Students should be aware that printing from personal technology devices will not be possible at school.

Students should not physically share their personal technology devices with other students.

A student's personal technology device may be searched by District personnel if there are "reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school."

Consequences for Violating the Student Responsible Use Policy

Misuse of District and personal technology resources on school property, in school vehicles and buses, at school-sponsored activities, as well as using District technology resources via off-campus remote access, may result in disciplinary action up to and including suspension, expulsion, or appropriate criminal or civil action. A violation may also result in a prohibition on the use and/or possession of personal technology on school property. This policy shall be used in conjunction with Bethel Board of Education policies and other local, state and federal laws and regulations.

Students, parents, and guardians should recognize that the nature of the use of District technology resources extends outside of the school itself and into off-campus remote locations such as homes. The District's jurisdiction to enforce student behavior and discipline policies and rules shall apply whether the misuse or violation is at school or away from school as long as the District's technology resources are being used in an inappropriate manner.

Legal Reference: Connecticut General Statutes

53a-182b. Harassment in the first degree: Class D felony. (as amended by PA95-143)
20 U.S.C. Section 6777, No Child Left Behind Act
20 U.S.C. 254 Children's Internet Protection Act of 2000
47 U.S.C. Children's Online Protection Act of 1998

Policy Approved: June 7, 1999
Policy Revised: 3/9/2004, 5/22/06, 5/10/07
6/28/11, August 21, 2012

SUFFIELD PUBLIC SCHOOLS
Suffield, CT

6141.321REG FORM

Student Responsible Use Agreement

Limitation of Liability

The District shall not be responsible for any damages suffered by the student, including those arising from unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the student's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The District assumes no liability for personal technology, including computers, SMART Phones, network access devices, or other electronic signaling devices if such devices are damaged, lost, or stolen. The student and his/her parent/guardian shall indemnify and hold The District harmless from any losses sustained as the result of misuse of the District's technology resources by the student, and/or the loss or damage of personal technology.

Agreement

I/We have read, understand, and will abide by the District's Student Responsible Use Policy, as described above. As a parent or guardian, I hereby consent to my child's or ward's use of the District's technology resources. I/We also agree to hold the District harmless for any damages suffered by my child/ward, including those arising from unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people arising from or connected to the use of the District technology resources.

Student User Name (Please Print): _____

Student User Signature: _____ Date: _____

Parent/Guardian Name (Please Print): _____

Parent/Guardian Signature: _____ Date: _____
(Parent/Guardian must sign if student user is under 18 years old.)

Please return this page of the Responsible Use Policy within one week.
If you have questions, please direct them to your school administrator. Thank you!