INSTRUCTION

Student Responsible Use Policy for Use of Region Technology Resources

Policy Statement

Region 12 Public Schools (the "Region") is pleased to offer students access to Region 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 Region and personal technology resources on school property, in school vehicles and buses, at school-sponsored activities, or using Region technology resources via off-campus remote access, each student must act in an appropriate, ethical manner consistent with school, Region, 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 Region 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 Region, students and their parents must sign the Region's Responsible Use Agreement acknowledging their responsibilities. Students must comply with all Region regulations and protocols to be permitted the use of Region technology resources.

The Region'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 Region grants access to its Region 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 Region 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 Region'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

Region Technology Resources:

For the purposes of the Region's BYOD policy, "Region Technology Resources" refers to Region's computers, Region issued personal data devices (including Smartphones, Blackberries, PDAs, 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 Region's BYOD 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 Region Technology Resources

In addition to the general principles set forth in this Student Responsible Use Policy, the use of Region 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:

1. The Region 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.

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

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

4. 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 Region network, or using the Region technology resources, any defamatory, abusive, obscene, profane, sexually-oriented, threatening, offensive, or illegal material. The use of Region 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.

5. Although the Region uses software filters to block known inappropriate web sites and prohibit access to harmful materials accessed from a Region network, the Region does not filter or block access to harmful materials accessed from Region-provided technology resources that are being used outside of the Region 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.

6. The use of the Region technology resources is not private. Students should not expect that files stored on or transmitted via the Region's resources will be confidential. All digital transmissions are subject to monitoring by Region employees and other officials. Digital storage is the Region's property, and as such, network administrators may review files and communications to maintain system integrity and ensure that students are using technology responsibly.

7. The Region denies any responsibility for the accuracy of information obtained from the Internet or on-line resources.

8. The Region makes no warranties of any kind, expressed or implied, for the technology resources it provides to students.

9. 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.

10. 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.

11. The use of Region 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 Region 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.

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

13. 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 Region 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 Region technology resources from personal technology is not available via hardwired connections.

Network Access by Students Using Personal Technology

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

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

- Students will access the Region's wireless network using their school account log-ins and passwords. Students are advised that the Region's network administrators have the capability to identify users and to monitor all BYOD devices while they are logged on to the network. As part of the monitoring and reviewing process, the Region will retain the capacity to bypass any individual password of a student or other user. *The Region technology security aspects, such as personal passwords and the message delete function for e-mail, can be bypassed for these purposes*. The Region'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 Region 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 BYOD 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 Region'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 Region 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 Region 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 Region and personal technology resources on school property, in school vehicles and buses, at school-sponsored activities, as well as using Region 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 Region 12 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 Region technology resources extends outside of the school itself and into off-campus remote locations such as homes. The Region'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 Region'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