

SEDGWICK SCHOOL COMMITTEE

POLICY NUMBER: 10.18

Adopted: 10/8/96

Previous Revision: 3/14/00, 10/16/07, 3/20/12

Revised: 9/17/19

STUDENT COMPUTER AND INTERNET USE

The Sedgwick School Committee provides computers, networks, and Internet access to support the educational mission of the school and to enhance the curriculum and learning opportunities for students and school staff. And as part of its commitment to ensure that all students are prepared for both college and modern, fulfilling careers, the schools have integrated 21st century technology into the curriculum.

The unregulated availability of information and communication on the Internet requires that the Committee establish reasonable controls for lawful, efficient and appropriate use of this technology.

- A. Student use of school computers, networks and Internet services is a privilege not a right. Students are required to comply with this policy and the school's rules. Students who violate the policy and/or rules may have their computer privileges revoked and may also be subject to further disciplinary and/or legal action. The principal shall have final authority to decide whether a student's privileges will be denied or revoked.
- B. As good digital citizens, students are not to engage in:
 - 1. Cyberbullying - the use of the Internet and related technologies to harass or harm other people in a deliberate, repeated, and hostile manner.
 - 2. Bypassing or interfering with the school's Internet filter.
 - 3. Accessing, creating, or distributing inappropriate content - including that which is obscene or threatening - which disrupts or interferes with the safety and welfare of the school community.
 - 4. Installing or removing any type of hardware or software on school-owned devices without permission.
 - 5. Damaging devices including, but not limited to, school computers, tablets, and network equipment. Repair costs for damaged school equipment will be billed to parents.
 - 6. Use of the school's network or electronic devices to download or host illegal content.
 - 7. Hacking - the act of accessing a device for which the hacker does not have permission from the owner, including using another user's password.
 - 8. Financial transactions - any activity involving an exchange of money.
- C. Failure to comply with the following acceptable use guidelines may result in loss of technology privileges and/or disciplinary action.

- D. All computers used in Sedgwick Elementary School are under the control, custody and supervision of the school. The school reserves the right to monitor all student use of computers and the Internet while on school property. Students have no expectation of privacy in their use of school computers.
- E. While reasonable precautions will be taken to supervise student use of the Internet, Sedgwick Elementary School cannot reasonably prevent all inappropriate uses, including access to objectionable materials and communication with persons outside of the school, in violation of Committee policies and school rules. Sedgwick Elementary School is not responsible for the accuracy or quality of information that students obtain through the Internet. However students will be taught to analyze a variety of information types and sources so that they may learn the skills needed as consumers of information. The technology staff will implement an Internet Safety educational program with lessons appropriate for students.
- F. Before a student is allowed to use school computers and Internet services, the student and the student's parent/guardian must sign and return the *Computer/Internet Access Acknowledgement*. The school will retain the signed acknowledgment.
- G. The Superintendent shall be responsible for overseeing the implementation of this policy including implementation of all applicable state and federal statutes and regulations. The Superintendent shall direct the development of additional administrative procedures/rules governing the day-to-day management, operation and supervision of Sedgwick Elementary School computer systems consistent with this policy. The Principal and other school staff shall be responsible for implementing school computer and Internet use rules.
- H. In compliance with the Children's Internet Protection Act (CIPA), it is the policy of the Sedgwick School Committee to: (1) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (2) prevent unauthorized access and other unlawful online activity; (3) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (4) comply with all other CIPA provisions.
 - 1. Access to Inappropriate Material - To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, other forms of electronic communications, and access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

2. Inappropriate Network Usage - To the extent practical, steps shall be taken to promote the safety and security of users when accessing electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

3. Digital Citizenship Training - The principal, technology coordinator and other school staff shall be responsible for providing age-appropriate digital citizenship training for students who use the school's digital technology. Training content will include appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.