Policy No. 00019

SIERRA CHARTER SCHOOL

STUDENT INTERNET USE POLICY AND AGREEMENT

Student Use of Technology

Sierra Charter School ("SCS") has adopted the Student Internet Use Policy and Agreement ("Policy") to ensure that student access to and use of the Internet is consistent with the educational goals and purposes of Sierra Charter School. SCS shall notify students and parents/guardians about authorized uses of school computers, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities.

Before using the school's on-line or technological resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement specifying user obligations and responsibilities. In the agreement, the student and his/her parent/guardian shall agree to not hold SCS responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They shall also agree to indemnify and hold harmless SCS and all school personnel for damages or costs incurred by users.

Definitions

"Educational Purpose" means classroom activities, research in academic subjects, career or professional development activities, school approved personal research activities, or other purposes as defined by SCS from time to time.

"Inappropriate Use" means a use that is inconsistent with an educational purpose or that is in clear violation of this Policy and Agreement.

Safety for On-Line Services/Internet Access

Sierra Charter School has taken precautions to restrict access to controversial materials with filters that block Internet access to websites that have no educational purpose and/or contain visual depictions of material deemed obscene, constitute child pornography, or to any material deemed harmful to minors. SCS shall ensure that all school computers with Internet access have a technology protection measure that blocks or filters Internet access to websites that have no educational purpose and/or contain visual depictions that are obscene, constitute child pornography, or that are harmful to minors. While SCS is able to exercise reasonable control over content created and purchased by SCS, it has limited control over content accessed via the Internet and no filtering system is 100% effective. Neither SCS nor its staff shall be responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence.

To reinforce these measures, the Principal or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision.

The Principal or designee also shall establish regulations to address the safety and security of students and student information when using email, chat rooms, and other forms of direct electronic communication.

The Principal or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, maintaining the student's online reputation and ensuring their personal safety by keeping their personal information private, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying. Students are expected to follow safe practices when using SCS technology.

Students shall not use the Internet to perform any illegal act or to help others perform illegal acts. Illegal acts include, but are not limited to, any activities in violation of local, state, and federal law and/or accessing information designed to further criminal or dangerous activities. Such information includes, but is not limited to, information that if acted upon could cause damage, present a danger, or cause disruption to SCS, other students, or the community. Damaging, debilitating or disabling computers, computer networks or systems through the intentional or overuse of electronic distribution or the spreading of computer viruses or other harmful programs shall be prohibited. Any unauthorized online access to other computers by means of hacking into other computers, downloading hacker tools such as port scanners and password crackers designed to evade restrictions shall also be strictly prohibited.

Student use of SCS computers to access social networking sites is not prohibited, but access is limited to educational purposes only. To the extent possible, the Principal or designee shall block access to such sites on SCS computers with Internet access.

The Principal or designee shall oversee the maintenance of SCS's technological resources and may establish guidelines and limits on their use.

All employees shall receive a copy of this Policy and Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All employees shall comply with this Policy and Agreement, in addition to any separate policies governing employee use of technology.

Student use of SCS computers, networks, and Internet services is a privilege, not a right. Compliance with SCS's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may have their computer privileges limited and may be subject to disciplinary action.

User Obligations and Responsibilities:

1. Use Limited to an Educational Purpose. SCS attempts to limit students of the Internet to only those activities that further or enhance the delivery of education. Under no circumstances are students permitted to use the Internet to access, download, or contribute to Internet sites that contain inappropriate content including, but not limited to gross, indecent, or sexually-oriented materials, gambling, or information related to violence or drugs.

2. Security. Students shall not impair the security of SCS's technology resources. Students are expected to:
   a. Safeguard all personal passwords. Students should not share passwords with others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised.

   b. Access technology only with their account or with a shared account as directed by their teacher and not to allow others to use their account or to use the accounts of others, with or without the account owner's authorization.

3. Authorized Use. Students may use SCS's technology resources when directed by a teacher, when technology has been designated for open student use (e.g., computers in the library), and for other educational purposes.

4. Plagiarism. Researching information and incorporating that information into a student's work is an acceptable educational use, but students must acknowledge the source of information. Plagiarism means the copying of a phrase, a sentence, a longer passage from a source, or any ideas written by someone else and claiming the written work as the student's original work. Student agrees that when using any information obtained on the Internet, he/she will acknowledge the source through quotation or academically accepted form of notation.

5. Copyright. Student agrees that he/she will not use the Internet to copy, retrieve, forward or send copyrighted materials including but not limited to print, text, music or pictures, unless the student has author's permission or is accessing a single copy only for the student's use.

6. Communication. Student agrees that he/she will not use school equipment or resource networks in the following manner:

   a. Student will not post on newsgroups or other message posting systems any communication containing profanity, racially disparaging remarks, or lewd and/or obscene language.

   b. Student will not at any time use speech that is not appropriate for an educational setting such as inflammatory language, profanity, personal attacks, harassment threats to do personal harm or other criminal activity, and language that is intended to be racially derogatory.

   c. Student will not place illegal information on the Internet, nor will student use the Internet in any way that violates federal, state, or local law.

   d. Student will not give out to any other Internet user or post on the Internet his/her name, address, or telephone number unless expressly authorized by the school in writing.

7. Disruptive Activity. Students shall not intentionally interfere with the performance of the school's network or intentionally damage any school technology resources.

8. Inappropriate Use. School technology, hardware, software, and bandwidth are shared and limited resources and all users have an obligation to use those resources responsibly. Students are provided access to SCS technology primarily for educational purposes. Students shall not use SCS technology or equipment for personal activities or for activities that violate SCS policy or local law. These include but are not limited to:
   a. Playing games or online gaming;
   b. Downloading software, music, movies, or other content in violation of licensing requirements, copyright, or other intellectual property rights;
   c. Installing software on SCS equipment without the permission of the Principal or designee or other authorized SCS staff person;
   d. Downloading, viewing, or sharing inappropriate content, including pornographic, defamatory, or otherwise offensive material;
   e. Conducting any activity that is in violation of SCS policy, the student code of conduct, or local, state, or federal law;
   f. Engaging in any activity that is harmful to other student(s), including the use of technology to harass, intimidate, bully, or otherwise disrupt the educational process;
   g. Participating in political activities;
   h. Conducting for-profit business;
   i. Using hacking tools on the network or intentionally introducing malicious code or viruses into SCS's network;
   j. Using any software or proxy service to obscure either the student's IP address or the sites that the student visits;

k. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering, or other security measures;
l. Accessing or attempting to access material or systems on the network that the student is not authorized to access.

9. Protection Measures. While SCS is able to exercise reasonable control over content created and purchased by SCS, it has limited control over content access via the Internet and no filtering system is 100% effective. Neither SCS nor its staff shall be responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. The student and parent agree not to hold SCS or any SCS staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They also agree to indemnify and hold harmless SCS and SCS personnel for any damages or costs incurred.

10. No Expectation of Privacy. The student acknowledges that computer equipment, Internet access networks, email accounts, and any other technology resources are owned by SCS and provided to students for educational purposes. SCS may require staff to monitor and supervise all access to computer equipment, Internet access networks, and email accounts. To facilitate monitoring of activities, computer screens may be positioned so that they are visible to the staff member supervising the students. Students have no right of privacy with respect to any messages or information created or maintained on Sierra Charter School's computers including Internet use, computer files, e-mails or other computer systems. SCS reserves the right to access stored computer records and communications, files, and/or other data stored on SCS equipment or sent over SCS networks to assure compliance with this Policy. Such computer records, communications, files, and data are not private and may be accessed during:

    a. Routine system maintenance.

    b. Inspection of SCS equipment at the end of the school year or agreed-to use period.

    c. Specific review of individual's files or monitoring of individual activity, when there is a reasonable suspicion that SCS is engaging in an inappropriate use.

11. Unauthorized Networks. Students may not create unauthorized wireless networks to access SCS's network. This includes establishing wireless access points, wireless routers, and open networks on personal devices.

12. Violation of Policy. The student acknowledges that violation of the Policy will subject the student to discipline, which may include loss of all Internet privileges or access and/or other appropriate disciplinary or legal action in accordance with the Student Code of Conduct, school disciplinary rules and policies, and applicable laws.

Student also acknowledges that SCS will contact the proper legal authorities if SCS concludes or suspects that the student's Internet activity is a violation of any law or otherwise constitutes an illegal activity.

After reading the above Policy, please complete the Agreement below to indicate you agree with the terms and conditions provided. The signature of both the student and parent/guardian are mandatory before access may be granted to the technologies available. This document, which incorporates both the Policy and the Agreement below, reflects the entire agreement and understanding of all parties.

ACKNOWLEDGEMENT OF THE TERMS OF SIERRA CHARTER SCHOOL'S INTERNET USE POLICY

I have read and understand the Student Internet Use Policy and Agreement and agree to abide by the terms and conditions that are set out in the Policy. I understand that computer use is a privilege and not a right. I understand if I violate this Policy in any way, I will be subject to a disciplinary referral. I understand that the parent or guardian of a minor student shall be liable for the replacement or repair cost of property that SCS has loaned to the student that the student fails to return or that is willfully cut, defaced, or otherwise damaged, up to an amount not to exceed ten thousand dollars ($10,000), adjusted annually for inflation.

_____ _____

Parent's/Guardian's Signature Date

_____ _____

Student's Signature Date

----------For School Employees Only----------

I have read, understand, and agree to abide by the Student Internet Use Policy and Agreement. I understand that SCS's policies, procedures, rules, and regulations which apply to students also apply to me as an adult user of SCS's technology, in addition to any separate policies governing employee use of technology.

Employee Signature: _____

Employee Name (Please Print): _____

Board Approved: 06/07/04
Board Amended: 03/12/07
Board Amended: 05/13/13
Board Amended: 05/12/15
Board Amended: 05/12/17