SCSC RESPONSIBLE USE OF TECHNOLOGY POLICY

It is the policy of the Seymour Community Schools (SCSC) Board of Education to provide electronic resources to students and staff for the purposes of
- promoting student achievement,
- supporting student and staff mastery of digital age skills*, and
- maximizing efficiency in corporate operations.

The SCSC Board of Education expects students and staff to utilize these resources in a manner consistent with this policy.

All SCSC students and staff are responsible for their actions and activities involving the school district's computers, electronic devices, network and Internet services, and for their computer files, passwords and accounts.

The rules and guidelines in this policy detail responsible use of electronic information resources under which students, staff, and all members of the SCSC community, herein referred to as "users," will be held accountable. The rules and guidelines outlined in this policy provide general guidance concerning the use of school computers and other electronic devices and provide examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity.

Students, parents, and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator. These rules apply to all school computers, all school-provided electronic devices wherever used, all uses of school servers, and Internet access and networks regardless of how they are accessed.

Responsible Use

1. School computers, network and Internet services, and electronic resources are provided for educational purposes and research consistent with SCSC's educational mission, curriculum and instructional goals.

2. Users must comply with all Board policies, the student handbook, and school rules and expectations concerning conduct and communications when using school computers or school- issued electronic resources, whether on or off school property.

3. Students also must comply with all specific instructions from school staff.

<u>Prohibited Use</u>

1. Accessing or Communicating Inappropriate Materials– Users may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. Illegal Activities– Users may not use the school district's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. SCSC and its employees assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources.

3. Violating Copyrights or Software Licenses– Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

4. Plagiarism–Users may not represent as their own work any materials obtained on the Internet (such as term papers, articles, music, etc). When using other sources, credit must be given to the copyright holder.

5. Use for Non-School-Related Purposes- SCSC's computers,electronic devices, networks and Internet services are provided for purposes related to educational programs, school operations, and performance of job responsibilities. Incidental personal use of school devices is permitted as long as such use: 1) does not interfere with the user's responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure or school rules. "Incidental personal use" is defined as use by an individual for occasional personal communications.

6. Misuse of Passwords/Unauthorized Access–Users may not share passwords; use other users' passwords; access or use other users' accounts; or attempt to circumvent network security systems.

7. Malicious Use/Vandalism–Users may not engage in any malicious use, disruption or harm to the school district's computers, electronic devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

8. Avoiding School Filters–Users may not attempt to or use any software, utilities or other means to access Internet sites or content blocked by the school filters.

9. Unauthorized Access to Blogs/Social Networking Sites, Etc. – Users may not access blogs, social networking sites, etc. prohibited by building administration or the SCSC Technology Department. Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.

10. Wasting System Resources - Users shall not use the network in such a way that would waste system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects, as determined by the supervising instructor or building administrator.

11. Unauthorized Equipment - Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district network without permission from the SCSC Technology Department.

Compensation for Losses, Costs and/or Damages

Users may be responsible for compensating SCSC for any losses, costs or damages incurred for violations of Board policies/procedures and school rules, including the cost of investigating such violations. SCSC assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, devices, or the school network.

Student and Staff Security

Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as web sites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.

Staff may post student pictures on district/ school/classroom "public" websites as long as the student's name or other identifying information is not included. Students' grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.

All Seymour Community Schools are closed campuses. SCSC retains all rights concerning any recording and/or publishing of any student's or staff member's work(s) or image(s). Students must obtain permission from a SCSC staff member to publish a photograph or video of any school- related activity. It is best practice and common courtesy to ask permission before recording an individual or groups. The use of cameras in any type of electronic device is strictly prohibited in locker rooms and restrooms.

SCSC staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

Students may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

Technology Privacy

All computers, telephone systems, voicemail systems, electronic mail, and electronic communication systems are the district's property. The district retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with district's computer system, telephone system, electronic mail system, and voice mail system. Students and staff should have no expectation that any information contained on such systems is confidential or private.

System Security

Any user who identifies a security problem must notify his/her teacher or building administrator immediately. The user shall not demonstrate the problem to others or access unauthorized material. Staff shall immediately report any potential security breaches to the SCSC Technology Department.

Personal Devices

All users are prohibited from using privately-owned electronic devices in school unless explicitly authorized by the building Principal or SCSC System Administrator.

Additional Rules for Chromebooks Issued to Students or Staff

1. Electronic devices loaned or leased to students or staff shall be used only for educational purposes that directly relate to a school project or assignment, unless otherwise explicitly authorized by building administration.

2. Users are responsible for the proper care of electronic devices at all times, whether on or off school property, including costs associated with repairing or replacing the device.

3. Users must report a lost or stolen device to the building administration immediately. If a device is stolen, a report also should be made immediately with local police.

4. The policy and rules apply to the use of the electronic device at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of devices issued by school staff.

5. Violation of policies or rules governing the use of electronic devices or any careless use of the device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies/ procedures or school rules.

6. Parents are responsible for supervising their student's use of the device when not in school.

7. The device configuration shall not be altered in any way by users. No software applications shall be installed, removed, or altered on the device unless permission is explicitly given by the teacher or building administrator.

8. The device is to be used only by the student or staff member to whom it is issued. The person to whom the device is issued will be responsible for any activity or action performed on the device.
9. The device must be returned in acceptable working order by the last day of each school year, upon withdrawal or exit date from the school district, and whenever requested by school staff.

Terms of Use

SCSC reserves the right to deny, revoke or suspend specific user privileges and/ or take other disciplinary action, including but not limited to student suspensions or

expulsion from school or staff suspensions or terminations, for violations of this policy. Additionally, all handbook regulations apply to the use of the SCSC network, Internet, and electronic resources.

Disclaimer – SCSC and its employees make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, SCSC is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.

2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.

3. Unauthorized financial obligations resulting from the use of SCSC electronic resources.

SCSC Responsible Use of Technology Policy - User Agreement

I understand and will abide by the above SCSC Responsible Use of Technology Policy. I further understand that any violation of the above regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked temporarily or permanently, discipline action may be taken, and appropriate legal action may be taken.

User's Full Printed Name _____

User's Signature _____

Date _____