Acceptable Use Policy

Sioux Center Christian School strives to carry out its mission statement in every program and curricular area. Thus, it is the policy of Sioux Center Christian School to:

(a) Monitor user access over its technology network to prevent transmission of inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
(b) Prevent unauthorized accesses and unlawful online activity;
(c) Prevent unauthorized disclosure, use, or dissemination of personal identification information of minors; and
(d) Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions:
Key terms are as defined in the Children's Internet Protection Act.
Access to Inappropriate Material:
SCCS employs hardware and software to block Internet access, or other forms of electronic communications, to inappropriate information for faculty and staff members and students. The hardware forms a firewall through which all Internet material must pass. The software includes a filter list that checks for and blocks objectionable sites.

The hardware and software blocks access to visual depictions deemed obscene, child pornography, and to any material deemed harmful to minors. In addition, it produces a report (log file) showing specific sites users have tried to visit and been blocked from. Only the system administrators can allow staff or students (minors) access to sites which the firewall blocks if the material is deemed appropriate and necessary for legitimate research or other lawful purposes.

Inappropriate Network Usage:
To the extent practicable, steps shall be taken to promote the safety and security of users of the SCCS online network when using email and other forms of direct electronic communications. Email is provided for faculty and staff members. Students in grades 4 through 8 are provided managed email accounts in order to share documents and school-related communication only. Network administrators are responsible for the management and monitoring of these accounts. Social networking and instant messaging sites are blocked for students and will only be allowed for educational purposes.

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.

Supervision and Monitoring:
It shall be the responsibility of all the members of the Sioux Center Christian School faculty and staff to supervise and monitor usage of the online network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Minors (students) are never permitted to have unsupervised technology access. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the network administrators.

Adoption:
The Acceptable Use Policy was adopted by the Board of Sioux Center Christian School on May 13, 2002. After review, it was updated in June 2015.

Internet access is available to students and employees at Sioux Center Christian School. We are pleased to have Internet access, as we believe it offers valuable, diverse, and unique resources to both students and teachers. Our goal in providing this service is to promote educational excellence in our school by facilitating resource sharing, innovation, and communication. We intend to use this tool to bring timely and useful information to employees and students. In summary, we want SCCS staff and students to use the Internet appropriately, thus

bringing praise to our God and creator.

With access to the Internet, and the availability of large quantities of material, concern for the protection of Christian values is crucial. Families should be warned that some material obtained online may contain items that are illegal, defamatory, inaccurate, or offensive. In order to minimize the risk of contact with controversial materials, SCCS employs technology that blocks many of these objectionable sites for students and staff members. The technology is updated each week to keep pace with new sites that are continually being made available. However, no blocking system is perfect. Because of this, students are never allowed to use the Internet at SCCS unless they are under the direct supervision of an SCCS faculty or staff member.

The purpose of this AUP for the SCCS network and the Internet is to set guidelines for the use of these resources that are consistent with our school mission statement, educational goals, and biblical principles. The smooth operation of the network relies on proper conduct by students and employees. Since SCCS has different groups of technology users—students and employees—who use Internet resources differently, the following guidelines are defined for each group:

Employees: Employees have Internet access through the SCCS network to obtain information that will enhance their work and help them grow professionally. Faculty and staff members' access will be limited by filtering. In addition, the network administrator will be allowed to check Internet history files and/or emails should the need arise.

Kindergarten through 3rd Grade Students (until 3rd graders have completed Internet training): Students in this category have not had formalized training on how to search Internet resources and keep personal information private. This formal training occurs as part of our 3rd grade curriculum. Students in these grades are only allowed to go to sites that have been specified by the SCCS faculty/staff member who is supervising the student's use of the Internet. This is usually accomplished by providing direct links from the teacher's website or the SCCS homepage. Students are not allowed to just search for information on their own. Students may search certain educational databases (such as the AEA Online resources) for information pertaining to an individual project since these sites are designed specifically for educational use. It should be noted that students are never permitted to "surf the web", since this is not a stewardly use of time.

3rd Grade (after obtaining Internet training) through 8th Grade Students: Since students in this category have earned their "Internet Driver License" by participating in specific instruction related to online safety and Internet research, they will be allowed to search the Internet and conduct individual research for projects that have been assigned by classroom teachers. Students are still not allowed to "surf the web". Also, students in this category must be under the supervision of an SCCS faculty or staff member when using the SCCS computer network.

General Terms and Conditions for SCCS Students

1. Students are responsible for good behavior on the school network and when using technology devices, just as they are in a classroom or hallway. General school rules for behavior and communication apply.

2. Students' Internet and technology use will be monitored by a teacher or staff member at all times.

3. Network access (including Internet access) is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Access is a privilege, not a right. Inappropriate use will result in a suspension or cancellation of Internet privileges. The following consequences will apply:

- First offense: The supervising teacher will talk with the student to ensure that he/she understands the nature of the offense. Network privileges may be suspended for the remainder of the school day, and parents will be notified by the supervising teacher.
- Second offense: The student will lose network privileges for one week. Parents will be notified by the supervising teacher.
- Third offense: The student will lose network privileges for one trimester of the school year. Parents

will be notified by the supervising teacher. Serious violations may result in immediate suspension of Internet privileges and may require the action and intervention of the head of school.

4. Users are expected to abide by universally accepted rules of network etiquette and conduct themselves in a responsible, ethical, and polite manner while online.

5. Users are not permitted to transmit, receive, submit, or publish any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material. Such offenses may be subject to the SCCS Anti-Bullying Policy, and action will be taken according to the guidelines that policy describes.

6. Physical or electronic tampering with computer resources is not permitted. Damaging devices, systems, or networks intentionally will result in cancellation of privileges.

7. Users must respect all copyright laws that protect authors, artists, software owners, and other owners of intellectual property. The SCCS Language Arts Curriculum explains how students will be instructed to properly document sources in grade-level appropriate ways. In accordance with this policy, staff members will both teach and model appropriate use of others' intellectual property. Plagiarism in any form will not be tolerated.

8. Security on any system is a high priority, especially when the system involves many users. If students can identify a security problem in the school's devices, network, or Internet connection, the students must notify the system administrator or their supervising teacher. Using someone else's password, or trespassing in another's folders, work, or files without written permission, is prohibited. Attempts to login to the Internet as anyone else may result in suspension of privileges in accordance with item #3 above.

9. SCCS makes no warranties of any kind, whether expressed or implied, for the service it is providing. We assume no responsibility or liability for any phone charges, line costs, or usage fees, nor for any damages a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions including those caused by user negligence, errors, or omissions. Use of any information obtained via the Internet is at your own risk. We specifically deny any responsibility for the accuracy of or quality of information obtained through Internet services.

10. All communications and information accessible via the technology resources shall be regarded as private property. However, administrators may review all files and messages to maintain system integrity and ensure that users are using the system responsibly. Messages relating to or in support of illegal activities may be reported to the authorities by the head of school.

11. Any violations of these guidelines may result in a loss of network privileges (as outlined in item #3 above), as well as other disciplinary or legal action that the head of school deems necessary. Users are considered subject to all local, state, and federal laws.