South Central Local Schools
Acceptable Use Policy and Internet Safety Agreement
2018-2019

Statement of Purpose

South Central Local Schools is pleased to offer our staff access to the World Wide Web and other electronic networks. The advantages afforded by the rich, digital resources available today through the World Wide Web outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved.

Terms of Agreement

In order for a staff to access a school computer system, computer network, and the Internet, staff members must sign and return the attached consent form

Acceptable Uses

The District is providing access to its school computer systems, computer networks, and the Internet for **educational purposes only**. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide. Accordingly, regulations for participation by anyone on the Internet shall include by not be limited to the following:

a) All users must abide by rules of Network etiquette – Netiquette, including the following:
   - Be polite. Use appropriate language and graphics. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
   - Avoid language and/or graphic representations which may be offensive to other users. Don't use network or Internet access to make, distribute, or redistribute jokes, stories, or other material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
   - Do not assume that a sender of email is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.

b) Teachers may allow individual students to use email, electronic chat rooms, instant messaging, social networking sites (I. E. facebook and myspace) and other forms of direct electronic communications for **educational purposes only** and with proper supervision. Proper supervision shall include the teachers having the documentation of the student's' username password on file and being able to monitor the account. This includes the use of student personal email accounts and personal social networking sites in the school environment. If a student uses his/her personal email account or accesses his/her social networking site on a school computer, the teacher must monitor all communications and have access to the student's username password for such account. In addition, if student personal accounts are access through the district Internet, the profile for student personal accounts must not contain identifiable information such as last name or address of student.

c) No personal addresses, personal phone numbers, or first names of students will be permitted to be given out on the Internet. No identifiable photographs will be allowed to be published on the Internet without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.

d) A student may not attempt to access any Internet resource without the prior consent of the teacher. The Internet is an extension of the classroom and teachers are responsible for and must be aware of where his/her student goes on the Internet.

Privacy. *Network and Internet access is provided as a* tool for your education. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.

e) **Student Photos/Student Work**. Publishing student pictures and work on websites promotes learning, collaboration and provides an opportunity to share the achievements of students. Images and products of K-12 students may be included on the website without identifying captions or names. Parents/guardians must indicate their written consent to publish their child's photo or school work on any school related website before the item is published to the web. Please note that under no circumstances will K-12 student photos or work be identified with first and last name on a district website, including the district, school, or teacher website.

Copyright. All students and faculty must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information.

Failure to Follow Acceptable Use Policy

Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network and Internet terminated and is subject to disciplinary action by the school administrator. The District may also take other disciplinary actions.

Unacceptable Uses of the Network may include:

a) Uses that cause harm to others or damage to their property. For example, do not engage in defamation (harming another's reputation by lies); do not employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; do not upload a worm, virus, Trojan horse, time bomb, or other harmful form of programming or vandalism; do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.

b) Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, do not disclose or share your password with others; do not impersonate another user.

c) Uses that are commercial transactions. Students may not use the SCS or school network to sell or buy anything over the Internet. You should not give others private information about yourself or others.

d) Illegal activities, including copyright or contract violations shall not be permitted on the Internet.

e) The Internet shall not be used for commercial, political, illegal, financial, or religious purposes. Violations shall be reported to a teacher or an administrator immediately.

f) Threatening, profane, harassing, or abusive language shall be forbidden.

g) Use of the network for any illegal activities is prohibited. Illegal activities include (a) tampering with computer hardware or software, (b) unauthorized entry into computers and files (hacking), (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under state and federal law. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

h) No user is permitted to knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.

i) Invading the privacy of another user, using another's account, posting personal messages without the author's consent, and sending or posting anonymous messages shall be forbidden.

j) Accessing pornographic or obscene materials, or using or sending profanity in messages shall be forbidden.

k) Any subscription to listservs, bulletin boards, or online services shall be approved by the superintendent or his designee prior to any such usage.

l) The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Internet Safety

- Parents and Users. Despite every effort for supervision and filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
- Personal Safety. In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.
- Confidentiality of Student Information. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
- Active Restriction Measures. The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The use of anonymous proxies to get around the content filter is strictly prohibited and will be considered a violation of this policy. The school will also monitor the online activities of students, through direct observation and/or technological means.

Use of New Web Tools

Online communication is critical to our students' learning of 21st Century Skills and tools such as blogging and podcasting offer an authentic, real-world vehicle for student expression. Again, as educators, our primary responsibility to students is their safety. Hence, expectations for classroom blog, student protected e-mail, podcast projects or other Web interactive use must follow all established Internet safety guidelines.

Blogging/Podcasting Terms and Conditions:

- The use of blogs, podcasts or other web 2.0 tools is considered an extension of your classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes but is not limited to profanity; racist, sexist or discriminatory remarks.
- Staff using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- A staff member should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
- Any personal blog a staff member creates in class is directly linked to the class blog which is typically linked to the staff profile, and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use that login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and follow these guidelines. Comments made on blogs should be monitored and - if they are inappropriate – deleted.
- Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
- Staff members using such tools agree to not share their username or password with anyone besides their teachers and parents and treat blog spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Staff members who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Teacher Responsibilities

- Will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district curriculum.
- All students will be informed of their rights and responsibilities as users of the district network prior to gaining access to that network, either as an individual user or as a member of a class or group.
- Use of networked resources will be in support of educational goals.
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy.
- Provide alternate activities for students who do not have permission to use the internet.

Principal Responsibilities

- Include Acceptable Use Policy in student handbook
- Be sure handbooks are distributed to all students
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy
- Permission forms must be kept on file for one year.
- Students who do not have permission to use the internet must be identified to the teaching staff.

District Responsibilities

- Ensure that filtering software is in use to block access to materials that are inappropriate, offensive, obscene, or contain pornography.
- Have acceptable use policy approved by the board and reviewed yearly.

South Central Local Schools

Acceptable Use Policy and Internet Safety 2018-2019

Consent Form

I have read and understand the Acceptable Use Policy and I agree to the following:

Staff Name (Please Print): _____

Staff email address : _____

Staff Signature: _____