Acceptable and Ethical Use of Technology Resources
Spearfish School District Network and Computer Systems

Definitions: The” District’s Computer Systems” and the “District’s Networks” are defined as any configuration of hardware and software, including all of the computer hardware, operating system software, application software, stored text, and data files. This also includes, but is not limited to, electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and any and all new technologies as they become available.

Policy: The use of the District’s Network, inclusive of the Wide Area Network (WAN) and the Local Area Network (LAN) is a privilege, not a right. Guidelines are provided to make all users aware of the responsibilities associated with educational, efficient, ethical, and lawful use of network resources. If a person violates any of these provisions, privileges may be terminated, access to the District Network may be denied, and the appropriate disciplinary action shall be applied. The District’s discipline policy shall be applied to student infractions.

In compliance with applicable laws, including SDCL 22-24-55, the District shall operate a technology protection measure that blocks or filters Internet access. The technology protection measure is intended to protect against access by adults and minors to content that is harmful to minors, abusive, obscene, profane, sexually explicit, threatening, illegal or pertaining to pornography, including child pornography. The District shall make reasonable efforts to restrict access to inappropriate materials and shall take reasonable measures to monitor the online activities of the end users; however, it is impossible to control all materials on a global network. Therefore, the District shall not be liable for the content or viewing of any materials not prepared by the District, or for access by a minor user to obscene materials under SDCL 22-24-57. Teachers may file a request with the Technology Coordinator to unblock websites that they believe have significant educational value. If the website is determined to be appropriate, the site will be unblocked.

Disciplinary action may be taken against students whose on-site communication causes a substantial disruption to the education environment or interferes with another student’s rights. Disciplinary action may also be taken against students for non-communication violations affecting the District’s Computer Systems and District’s Networks. Criminal action by law enforcement authorities may be taken against students if their on-site communication constitutes a threat or otherwise constitutes illegal conduct.

The parent/guardian shall notify building administrators each year if the parent/guardian does not want his or her child to independently use the District’s Computer Systems to access the Internet. Unless the District receives a proper authorization from the student and parent/guardian, students will not be permitted Internet access (See Code 6245). If a parent/guardian denies Internet access, this does not apply to direct classroom instruction where the teacher uses the Internet as a classroom demonstration or in a situation where the students are using computers and being supervised by District staff in the directed use of specific Internet sites as part of the class curriculum. Teachers should be prepared to provide alternate activities for students who have lost privileges through disciplinary action.

User accounts are considered the property of the District. The District expressly reserves the right at any time to review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted, reporting any violation to the school administration or law enforcement officials.

Persons using the District's Computer Systems or District's Networks shall have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent, received, or stored on the District's Computer Systems or District's Network.

The District does not guarantee that the District's Computer Systems or District's Networks will be uninterrupted or error-free; nor does it make any warranty as to the results to be obtained from use of the service or the accuracy or quality of the information obtained on or by them. **Access to the District's Computer Systems or District's Network is provided on an "as is" basis without warranties of any kind, express or implied, and all implied warranties including those of merchantability or fitness for a particular purpose are excluded. Neither the District nor any of its agents or employees shall be liable for any direct, indirect, incidental, special, or consequential damages arising out of the use of or inability to use the District's Computer Systems or District's Network or out of any breach of any warranty, express or implied.**

Security of all networks connected to the District is a high priority. Anyone observing a security problem on the District's Computer Systems or District's Network shall notify District personnel. Any person identified as a security risk or having a history of problems with other computer systems may be denied access to the District's Computer Systems or District's Network.

The District's Network may not be used for personal gain, which includes District email and/or web pages, to solicit sales or conduct business.

Proper Use of District Network and Computer Systems
Proper use of the District's Computer Systems and the District's Network requires that District staff and students abide by the following guidelines. District staff and students shall:

(a) be responsible for all use of the network under their accounts, regardless of whether access is gained with or without the person's knowledge and/or consent;
(b) immediately notify the District if the person suspects any unauthorized use of their account. The person shall remain liable and responsible for any unauthorized use until the District is notified of the suspected unauthorized use and the District has a reasonable opportunity to act upon such notice;
(c) be responsible for any costs, fees, charges, or expenses incurred under the person's account number in connection with the use of the the District's Computer Systems and the District's Network except such costs, fees, charges, and expenses as the District explicitly agrees to pay;

(d) avoid anonymity when communicating through electronic resources, unless authorized by the District or completing professionally-related surveys;
(e) ensure that student information shared electronically complies with the Family Educational Rights and Privacy Act;
(f) delete non-District authorized or adopted software if disk-space or system conflict issues arise;
(g) abide by all District policies and regulations when accessing personal email accounts, chat rooms, social networking sites or other forms of direct electronic communications via the District's Network;
(h) not send, access, or retain any abusive, defamatory, obscene, profane, sexually explicit, pornographic, threatening, or illegal material;
(i) not transmit copyrighted material without the express consent or authorization of the owner of the copyrights;
(j) not disclose passwords;
(k) not intentionally damage the District's Computer Systems, equipment or software or intentionally attempt to harm or destroy data of another person. This includes, but is not limited to, "hacking" and the loading or creation of computer viruses. The persons responsible for such actions or their parents/guardians shall be responsible for damages or the cost of correcting the problem;
(l) not install equipment on or make modifications to the District's Computer Systems or District's Network without pre-authorization from the District Technology Coordinator;
(m) not utilize proxy sites or other means to circumvent the District's filter;
(n) not include in student folders executable files (*.exe), batch files (*.bat), command files (*.com), system files (*.sys), media player files (*.mp3), or network files unless the file(s) directly relate(s) to a classroom assignment;

Educational Use of District Technology Resources

Online communication and network resources are an important part of 21st Century teaching and learning. The network and technology resources are considered an extension of the classroom. An educator's role includes fostering development of students who are reasonably equipped to communicate effectively, ethically and safely through appropriate guidance to students using telecommunications and electronic information resources related to the District curriculum. Teachers may allow students to use forms of online collaboration such as email, wikis and blogs, etc. for educational purposes only and with proper supervision. Proper supervision shall include the teacher having documentation of the identities of participating students and being able to monitor the account. Spearfish School District or designated representatives will provide age-appropriate training on educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Ethical Use of District, Public, or Private Technology Resources

Ethical behavior requires that District staff and students show consideration and respect whenever using computers or electronic communication/technology/devices/resources. When

interacting with each other, District staff and students shall:

(a) not include in electronic communication between staff, students and/or parents/guardians, comments or content that would not be acceptable in a face-to-face communication;

(b) not disclose, use, or disseminate unauthorized personal information of another person;

(c) distinguish between personal social networking sites and professional social networking sites. *"Social networking" is any form of Internet-based publication or presence where interactive communication is permitted, which includes social networks, blogs, Internet websites, Internet forums, and wikis, with examples including: Facebook, Twitter, YouTube, Google+, and Flickr. "Professional social networking" means work-related social media designed to address professional development, instructional, educational or extra-curricular program matters, and where communication is treated with the same professionalism as in a classroom or other employment setting. "Personal social networking" means non work-related social networking for the user's own personal use. Staff members shall limit their access to only professional social networking sites when they are at work.* Staff shall not invite or accept current District students, except for the staff person's relatives, into any personal social networking sites; and

(d) evaluate all information for its accuracy, reliability, and authority.

Disciplinary action may be taken against staff or students whose off-site communication causes a substantial disruption to the education environment or substantially interferes with another's rights. Criminal action by law enforcement authorities may be taken if the off-site communication constitutes a threat or otherwise constitutes illegal conduct.

Adopted	January 10, 2011
Revised	November 12, 2012
Revised	May 8, 2017