

Student Use of the Internet and Electronic Communications

Terms and Conditions for In-School Use of Internet Resources Big Sandy School District 100J

The Big Sandy School District 100J offers World Wide Web internet access to your child at his/her school. This access offers vast, diverse, and unique resources and is provided to students and school personnel to promote educational excellence in Simla Schools. The purpose of this document is to inform parents, guardians, and students of the availability of the internet resources as well as the rules governing its use and to obtain express parental or guardian permission for an individual student to use the internet while at school

The internet is an electronic highway connecting thousands of computers all over the world which can give students and teachers access to a variety of rich, educational resources. The World Wide Web, a portion of the internet that your student can use, includes some information specifically designed for children, up-to-the-minute scientific information, Supreme Court documents, and other information that is traditionally difficult to obtain in the school environment. To access the World Wide Web at school students will be using a World Wide Web browser (a piece of software) called Microsoft Explorer or something similar. This allows students to navigate through "web" information by pointing and clicking the mouse. Information is presented richly in text, pictures, sound and some video. Students can send electronic mail through Microsoft Explorer or something similar, but the access described in this document will not provide students with their own internet e-mail address, the ability to create World Wide Web pages, or the ability to access the internet from home.

The educational value of appropriate information on the internet is substantial. The internet is composed of information provided by institutions and people all over the world and thus, also includes material that is not of educational value in the context of the school setting. There is information which may be judged as inaccurate, abusive, profane, sexually oriented or illegal. Big Sandy School District does not condone or permit the use of this material. It is a joint responsibility of school personnel and the parents or guardian of each student to educate the student about his or her responsibility when using the internet. One of our school goals is to support students in responsible use of this vast reservoir of information. In addition to student education, internet access is available to students on computers that are in highly traveled areas of the school building such as classrooms, computer laboratories and the media center. However, parents and guardians must be aware that while in school, direct supervision by school personnel of each student using the computers is not always possible. Thus, students are expected to use the resources in a manner consistent with the contract and will be held responsible for their use. Additionally, parents should discuss with their children their own expectations for their child's internet use.

The following rules have been established to preserve the operation and integrity of Big Sandy Schools' computer network. These rules will coexist with any and all other rules established for this learning institution. They will be severely enforced and monitored.

1. No loading any programs without written permission from the technology teachers.
2. No using any unauthorized program. These include, but are not limited to, programs that have been loaded without permission and administrative programs.
3. Do not attempt to login under any other user other than yourself.
4. Do not delete any program or system files without permission from the technology teachers.
5. Do not put any obscene or offensive material on computers. This includes, but is not limited to, wall paper (backgrounds) or screensaver messages on computers.
6. Do not attempt to gain unauthorized access to any file server and/or computer that you do not have permission for.
7. Any file(s) saved on any computer or file server is the property of Big Sandy Schools, and can be accessed by school administration.
8. Do not attempt to delete, destroy, or modify other user's files. This includes, but is not limited to, files belonging to students, teachers or users.
9. Do not attempt to install, view, or download pornographic material of any kind. No exceptions! This includes, but is not limited to, pictures, games, and text files.
10. Do not vandalize school property.
11. Do not "play tricks" on other users. (hiding files or icons, mouse setting, etc.).
12. Do not attempt to modify any system settings. (CMOS settings, BIOS settings, etc.)
13. Obey any rules set by teachers or administrators. Flash drives allowed by teacher approval only.
14. Inform the technology teachers, or other administrative personnel of violations or problems with computers.
15. No sending messages across the network (msn Live, Google chat).
16. Do not give your password out to anyone. You will be held responsible for any misuse of your account. Your e-mail account will be accessed once a day.
17. No e-mail unless otherwise approved by teacher.
18. The sharing of electronic classroom files is prohibited unless approved by the teacher.

Violation of any of the above rules can/will result in suspension, expulsion, criminal prosecution, and/or banning of the violator's computer access. The banning of access can/will result in receiving failing grades for classes that require computer access. This policy is subject to change without notice.

The Internet and electronic communications (e-mail, chat rooms and other forms of electronic communication) have vast potential to support curriculum and student learning. The Board of Education believes they should be used in schools as a learning resource to educate and to inform.

Use of the Internet and electronic communications require students to think critically, analyze information, write clearly, use problem-solving skills, and hone computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals, and locate material to meet educational and personal information needs.

The Internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to students. While it is impossible to predict with certainty what information students might locate or come into contact with, the district shall take reasonable steps to protect students from accessing material and information that is obscene, child pornography or otherwise harmful to minors, as defined by the Board. Students shall take responsibility for their own use of district technology devices to avoid contact with material or information that may be harmful to minors.

Blocking or filtering obscene, pornographic and harmful information

Technology that blocks or filters material and information that is obscene, child pornography or otherwise harmful to minors, as defined by the Board, shall be installed on each technology device provided by the district that allows for access to the Internet by a minor, from any location. Students shall report access to material and information that is obscene, child pornography, harmful to minors or otherwise in violation of this policy to the supervising staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.

No expectation of privacy

District technology devices are owned by the district and are intended for educational purposes at all times. Students shall have no expectation of privacy when using the Internet or electronic communications. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district technology devices, including all Internet and electronic communications access and transmission/receipt of materials and information. All

material and information accessed/received through district technology devices shall remain the property of the school district.

Unauthorized and unacceptable uses

Students shall use district technology devices in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of district technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following.

(Note: The Board has discretion to determine which uses are unacceptable. The following list provides examples the Board may wish to consider.)

No student shall access, create, transmit, retransmit or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
- that is not related to district education objectives
- that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the district's nondiscrimination policies
- for personal profit, financial gain, advertising, commercial transaction or political purposes
- that plagiarizes the work of another without express consent
- that uses inappropriate or profane language likely to be offensive to others in the school community
- that is knowingly false or could be construed as intending to purposely damage another person's reputation
- in violation of any federal or state law or district policy, including but not limited to copyrighted material and material protected by trade secret

- that contains personal information about themselves or others, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account without written permission from that individual
- that impersonates another or transmits through an anonymous remailer
- that accesses fee services without specific permission from the system administrator

Security

Security on district technology devices is a high priority. Students who identify a security problem while using the Internet or electronic communications must immediately notify a system administrator. Students should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use another person's password or any other identifier
- gain or attempt to gain unauthorized access to district technology devices
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users

Any user identified as a security risk, or as having a history of problems with other technology, may be denied access to the Internet and electronic communications.

Safety

In the interest of student safety, the district shall educate students [Optional language: and parents] about appropriate online behavior, including cyberbullying awareness and response, interacting on social networking sites and in chat rooms, and other forms of direct electronic communications.

Students shall not reveal personal information, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate him or her. Students shall not arrange face-to-face meetings with people met on the Internet or through electronic communications.

Vandalism

Vandalism will result in cancellation of privileges and may result in school disciplinary action, including suspension or expulsion, and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt operation of any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district-owned technology device. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized software

Students are prohibited from using or possessing any software applications, mobile apps or other content that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees.

Assigning student projects and monitoring student use

The district will make reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

Opportunities shall be made available on a regular basis for parents to observe student use of the Internet and electronic communications in schools.

All students shall be adequately supervised by staff while using the Internet or electronic communications. Staff members assigned to supervise student use shall have received training in Internet and electronic communications safety and monitoring student use.

Student use is a privilege

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy shall result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in school disciplinary action, including suspension or expulsion,

and/or legal action. The school district may deny, revoke or suspend access to district technology or close accounts at any time.

Students and parents/guardians shall be required to sign the district's Acceptable Use Agreement annually before Internet or electronic communications accounts shall be issued or access shall be allowed.

School district makes no warranties

The school district makes no warranties of any kind, whether express or implied, related to the use of district technology, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the district of the content, nor does the district make any guarantee as to the accuracy or quality of information received. The district shall not be responsible for any damages, losses or costs a student suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the student's own risk.

BYOT (Bring your own technology)

Access to the District's wireless network, including the Internet, shall be made available to students, employees and members of the Board of Education primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

- Imposes no tangible cost to the District;
- Does not unduly burden the District's computer or network resources;
- Has no adverse effect on an employee's job performance or on a student's academic performance.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies.

Guest access to Wi-Fi is available at school functions; the school is not responsible for content and usage.

Unauthorized recording

Conversations and communications should generally be free and open between students, parents, employees and others. Surreptitious recording of conversations detracts from appropriate levels of trust needed for the effective operation of the school district and exposes the school district to potential breaches of confidentiality.

Toward this goal, all persons are prohibited from recording or reproducing, via any recording device, any conversation or communication between students, parents, employees or others while on school district premises, while conducting school district business or at school related activities, without the express written or oral consent of all persons engaged in the conversation or communication, or without the permission of the appropriate administrator or the superintendent.

Communications include, but are not limited to, statements made or images recorded during classes, school activities, meetings, hearings, conferences, counseling sessions, or other communications between students, parents, employees or others. Communications also include telephonic communication, including cellular phone communications.

Recording devices include, but are not limited to tape recorders, cell phones, cassette tape recorders, video recorders, digital recorders, or any other device which is capable of recording communications.

This does not prohibit the recording or reproducing of communications where all persons involved are aware that the communication is being recorded and all persons give their informed consent to have the communications recorded either in writing or through participation.

This does not prohibit appropriate school district officials from recording hearings, grievances, official investigations or images from security cameras.

This does not prohibit photographing or video recording appropriate public portions of school activities and athletic events where such photographing or video recording is customary and allowed.

Any employee who violates this agreement shall be subject to discipline up to and including termination or a recommendation for dismissal. Any student who violates this policy shall be subject to discipline up to and including long term suspension or expulsion.

Students may not employ the photographic, video-graphic, audio recording or reproduction capacity of any electronic device for the purposes of photographing, video capture, recording or reproduction of the same of any student or staff person without the express consent of the staff person, or under the supervision of a teacher or administrator. This section applies at all times while on school premises including school buses or at school sponsored events, regardless of the location.

Adopted: October 2, 2002
Revised and recoded: May 18, 2011
Revised: November 2012
Adopted: December 5, 2012
Revised: February 17, 2016
Adopted: March 30, 2016

LEGAL REFS.: 20 U.S.C. 6751 *et seq.* (*Enhancing Education Through Technology Act of 2001*)
47 U.S.C. 254(h) (*Children's Internet Protection Act of 2000*)
47 C.F.R. Part 54, Subpart F (*Universal Support for Schools and Libraries*)
C.R.S. 22-87-101 *et seq.* (*Children's Internet Protection Act*)

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
EGAEA, Electronic Communication
JB, Equal Educational Opportunities

Big Sandy School District 100-J, Simla, Colorado