

Board Policy Document

STUDENT PERSONNEL

Series 500

Policy Title: Computer Networks Acceptable Use Policy

Code Number: 581.12

Sioux City Community School District Policy on District-Provided Access to Electronic Information, Services, and Networks

General

The Sioux City Community School District provides electronic network communications for educational use by students. The purpose is to assist the District in meeting its educational mission, goals and objectives. Board Policy 603.10 requires that all materials be consistent with District-adopted guides, supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students. The communications include but are not limited to e-mail and the Internet. The Network shall be used for curriculum support purposes only. It is the policy of the District that all computer services shall be used in a responsible, efficient, ethical and legal manner.

No person shall access the District network with non-District hardware without approval of the Technology Department. Non-District hardware includes, but is not limited to, personal computers (laptop or desktop), wireless access devices and handheld devices.

The use of the network is a privilege, not a right, and may be revoked with or without notice and with or without cause at the discretion of the District. Failure to follow processes and procedures or abuse of resources may result in loss of privileges and possible disciplinary action.

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays or other service interruptions caused by either the district or user's own negligence, errors or omissions. Use of any information obtained via the District network is at the user's own risk.

First Adoption: January 27, 1998
Revision Adoption: March 13, 2006/February 23, 2009
Legal Reference:

Board Policy Document

Users should not expect that files stored on the Network or school-based computers will be private. Electronic messages, network activities, and files may be reviewed to maintain system performance, integrity, to insure that users are acting responsibly, and for any other purpose at the discretion of the District.

Access to the District's network is provided via an assigned user and ID and password for students in certain grades. It is the responsibility of the student to maintain the privacy of their password. Use of District information technology systems implies consent to monitoring for such purposes.

Internet

The Board believes that the Internet can be a valuable educational and productive tool that enables students to explore thousands of libraries, databases, bulletin boards, and other resources. However, families should be aware that some material accessible via the Internet may contain information that is illegal, defamatory, inaccurate or potentially offensive.

State and Federal mandates require schools to restrict access to certain information on the Internet, and the District will strive to provide a safe, quality Internet experience for both students and staff. District employees may monitor student Internet activity and blend thoughtful use of the Internet into the curriculum. Parents, however, should be aware that in spite of District safeguards, a student may still find ways, intentionally or unintentionally, to access inappropriate material.

The Board believes that all network services (e.g., computers, E-mail, Internet access) are a valuable part of the total program in that they promote educational excellence. At the same time, the Board believes that access to these services entails responsibility and that all computer services shall be used in a responsible, efficient, ethical and legal manner. General school rules for behavior apply.

The following uses of school-provided Network access are prohibited (collectively "Prohibited Uses"):

- a. To access, upload, download, or distribute pornographic, obscene, or sexually explicit material;
- b. To transmit obscene, abusive, sexually explicit, or threatening language;
- c. To violate any local, state, or federal statute;
- d. To vandalize, damage, or disable the property of another individual or organization;
- e. To access another individual's materials, information or files without permission;
- f. To access "personal" e-mail accounts;

First Adoption: January 27, 1998
Revision Adoption: March 13, 2006/February 23, 2009
Legal Reference:

Board Policy Document

- g. To access internet gaming sites;
- h. To access any social media sites such as Twitter, Facebook, MySpace, YouTube, blogs, and wikis, etc.
- i. To use instant messaging;
- j. To use streaming audio or video sites unless approved for curriculum use;
- k. To use non-District hardware or devices on the District network;
- l. To connect to wireless Access Points not supported by the District;
- m. To install any unauthorized software;
- n. To install or remove any computer hardware components from District computers (e.g. memory, optical drives, etc.);
- o. To violate copyright or otherwise use the intellectual property of another individual or organization without permission; and
- p. To engage any other inappropriate uses as determined by the District.
- q. Students shall NOT use proxy software to bypass district filters

E-Mail

Students at certain grades levels will be issued a District-provided email account. District-provided student email will be used solely for school related work, activities, and functions; any other use is strictly prohibited. Students shall not access non-District email via the Internet at school. All Prohibited Uses outlined for the Internet above apply to the use of District-provided student email accounts. Additionally, the following guidelines apply to your use of your District-provided email account:

- Students are responsible for keeping their passwords private. Students will not share passwords with anyone other than parents, a teacher, or the District's technology department. Never distribute passwords to anyone via email.
- Students shall not divulge personal information such as social security number or other sensitive or confidential information.
- Students who receive email that contains inappropriate content, or violates the Prohibited Uses policy should notify a teacher, principal, or parent immediately.
- Any form of cyber bullying or harassment will not be tolerated. Students who are the victim of cyber bullying or harassment should immediately report it to a teacher or principal. All reports of cyber bullying or harassment will be investigated by the District.
- Do not use District-provided student email to forward jokes, chain letters, pictures, or other inappropriate material as outlined in the previous section.

Board Policy Document

File Storage on District Network

Students in certain grades will be granted access to District file servers to store coursework and related educational content in a central site that is secure and periodically backed up. The following types of files are not acceptable for storage on district file shares:

- Audio files such as mp3s, AAC or others
- Video files such as .mp4, .swf or others
- .EXE files for non education related software
- Games, game emulators, game related files
- Any program related to a prohibited use such as proxy software
- Personal or confidential information

The above programs will be deleted from student folders without warning. Audio files that may be necessary for curriculum purposes should be kept on personal storage or handled by a teacher. Continued abuses of file storage may result in loss of network privileges and be subject to discipline.

Student Procedure for the Non-Directed Use of the Internet

Subject to this policy and monitoring by the District, all students will be granted independent use of the District's link to the Internet unless the District is notified by a parent or guardian as to the contrary. Annually, if a parent or guardian of a student wants to opt out of the independent use of the Internet for the forthcoming school year, they must submit an Internet Non-Authorization form signed by the parent/guardian notifying building administrators that the parent/guardian *does not* want his or her child to *independently* use the Internet. These forms will be kept in the office with the Student Permanent Record, and building staff will be notified of these students. This does not apply to classroom instruction where teachers will suggest appropriate sites and supervise the use of the Internet as a direct part of the curriculum.

Internet Based Social Media Use Within the District

The District reserves the right to remove fans/followers from its social media pages for any lawful reason including, without limitation, content that violates District policy. The District may amend this social media policy at any time and it is the fans'/followers' responsibility to review changes to this policy. By participating on the District's social media sites, depending on personal account and privacy settings, individuals may be subject to having their profile picture, name and comments visible to the public. The District does not take responsibility for such actions.

COPPA

First Adoption: January 27, 1998
Revision Adoption: March 13, 2006/February 23, 2009
Legal Reference:

Board Policy Document

Because we care about the safety and privacy of children online, the District complies with the Children's Online Privacy Protection Act of 1998 (COPPA). COPPA and its accompanying FTC regulation establish United States federal law that protects the privacy of children using the Internet. The District's site is not intended to solicit information of any kind from children under 13. It is possible that by fraud or deception the District may receive information pertaining to children under 13. If notified of this, as soon as the information is verified, the District will immediately obtain parental consent or otherwise delete the information from District servers.

Disciplinary Actions

Violations of this policy are subject to disciplinary action, up to and including expulsion from school. To ensure that the use of the District's information system and other electronic communications systems is consistent with the District's educational and legitimate business interests, authorized representatives of the District may monitor the use of such equipment.

See Board Policies, 603.10, and 603.11 (AR603.11).