

Student Acceptable Use Policy for Steelton-Highspire School District Network Access (CIPA Compliance): Computer Use

Telecommunications is radically changing the way the world accesses information. A computer network, linked to the Internet, an international computer network made up of many contributing networks, represents a powerful educational resource unlike anything that precedes it.

Using Internet resources both locally and world-wide users can:

- Access research materials to meet their educational and personal information needs.
- Consult with experts in various content area and unified arts fields.
- Connect with university and college libraries.
- Communicate directly with other users locally or world-wide.
- Engage in electronic "field trips."

The skills required for using a computer network and the Internet are vital to the long-term success of users when they enter higher education and the work force. Steelton-Highspire School District (SHSD) is pleased to offer its students access to its computer network (the SHSD Network) and the Internet to enhance and support student learning.

SHSD is aware that the Internet is an unregulated communication environment in which information changes constantly, and that some of this information may be inappropriate for users, based on age and/or development levels. SHSD's educators will take an active role in ensuring that students and their parents are aware of the individual user's responsibility in using the Internet resources in an ethical and educational manner. SHSD's goal is to provide individual users with the understanding and skills needed to use the Internet in ways appropriate to their individual educational needs.

SHSD will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

SHSD has developed the following policy regarding the acceptable use of its network and the Internet to establish each user student's rights and responsibilities as well as to delineate certain prohibited activities.

Rights

Members of the SHSD Network community have certain privileges and rights. Infringement of or disrespect to the rights of others may result in the loss of your network privileges.

1. Privacy/Monitoring Notification - All computer communication systems, and all communications and stored information transmitted, received, or contained in the SHSD Network's systems are SHSD's property and are to be used by students only for school-related purposes. All student members of the SHSD Network community have the right to privacy in their private electronic communications with respect to other students. However, to ensure proper use of the SHSD Network, SHSD may monitor the use of the SHSD Network from time to time. This monitoring may include accessing a student's private correspondence or files. In the event there is a reasonable suspicion that a user is using the SHSD Network in violation of the guidelines

stated in this policy, a system administrator or teacher may gain access to a student's private correspondence or files without prior notice. System administrators also may need to access private files as part of regular system maintenance.

2. Equal Access - All members of the network community will be granted free and equal access to as many network services as their technology allows. Exploration of the Internet is encouraged relative to the purposes of the SHSD Network. However, no single user should monopolize a computer or the network it uses. You may be asked to remove personal files if total system storage space becomes low.
3. Safety - To the greatest extent possible, members of the SHSD Network community will be protected from harassment or unwanted or unsolicited contact. Any community member who receives threatening or unwelcome communications should bring them to the attention of a system administrator or teacher. Users must, however, be aware that there are many services available on the Internet that could potentially be offensive to certain groups of users. The Administrators of the SHSD Network cannot eliminate access to all such services, nor could they even begin to identify all of them. Thus, individual users must take responsibility for their own actions in navigating the Internet.
4. Intellectual Freedom - The SHSD Network must be a free and open forum for expression, including viewpoints that are strange, unorthodox or unpopular. However, the poster of an opinion should be aware that others may be openly critical of such opinions. Occasionally, a message that you post may be met with especially harsh criticism (a practice known as "flaming" or "slamming"). It is best not to respond to such attacks, unless you believe you are capable of a measured, rational reply. Personal attacks are not an acceptable use of the SHSD Network at any time. SHSD does not officially endorse any opinions stated on the SHSD Network. Any statement of personal belief is implicitly understood to be representative of the author's individual point of view, and not that of SHSD as a whole.

Responsibilities

With the rights of membership in the SHSD Network community come certain responsibilities. Users need to familiarize themselves with the responsibilities. Failure to adhere to them may result in the loss of SHSD Network privileges.

1. Never share your password or account with anyone. You have full responsibility for the use of your account. All violations of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should you give your password to another user.
2. Do not knowingly degrade the performance of the SHSD Network. Electronic chain letters and mail bombs are prohibited for this reason. The creation, and/or distribution of destructive software, including, but not limited to, virus', trojanhorse, and worm programs, is strictly prohibited.
3. Obey the rules of copyright. SHSD Network community members must respect all copyright issues regarding software, information, and attributions of authorship. Commercial software may not be installed on the system without the express permission of the system administrators.
4. Posting personal communications to a public forum without the original author's prior consent is prohibited. To do this is a violation of the author's privacy. However, all messages posted in a public forum such as newsgroups or aliased e-mail may be copied in subsequent communications, so long as proper attribution is given.
5. Use of the SHSD Network for any illegal activities is prohibited. Illegal activities include tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or

destruction of computer files. Such activity is considered a crime under state and federal law.

6. Avoid the knowing or inadvertent spread of computer viruses. "Computer viruses" are programs that have been developed as pranks and can destroy valuable programs and data. Deliberate attempts to degrade or disrupt system performance of the SHSD Network or any other computer system or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law.
7. Use appropriate language. Profanity or obscenity will not be tolerated on the SHSD Network. All community members should use language appropriate for school situations as indicated by school codes of conduct.
8. Avoid offensive or inflammatory speech. Community members must respect the rights of others both in the local community and in the Internet at large. Personal attacks are unacceptable use of the SHSD Network. If you are the victim of a "flame" or "slam," bring the incident to the attention of a teacher or system administrator.
9. Impersonations, anonymity, aliases or pseudonyms are not permitted. As an educational network, we believe that individuals must take responsibility for their actions and words.
10. Exemplary behavior is expected on "virtual" field trips. When "visiting" locations on the Internet, or using the videoconferencing or screen sharing communication tools, community members must conduct themselves as representatives of both their class and the entire community as a whole. Conduct that is in conflict with the responsibilities outlined in this document will be subject to loss of SHSD Network privileges.

**Access to
Inappropriate
Materials**

To the extent practical, technology protection measures (or "Internet filters") have been implemented to block or filter Internet content or other forms of electronic communications that is inappropriate for the stated educational goals and objectives of the District.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled, or in the case of minors, minimized only for pre-approved bona fide educational research or other lawful purposes that are in accordance with the District's educational goals and objectives.

**Network Etiquette
and Privacy**

An SHSD Network user is expected to follow the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite.
2. Never send or encourage others to send abusive messages.
3. Use appropriate language. Remember that the user is a representative of his/her school. What is written can be viewed world-wide! Never swear, use offensive or obscene words, or any other inappropriate language.
4. Privacy. Users should never reveal their names, home addresses and personal phone numbers nor the names, addresses and phone numbers of any other person.
5. Electronic mail. Electronic mail is not guaranteed to be private. Messages relating to, or in support of, illegal activities must be reported to the system administrator or a teacher.

6. Disruptions. Users must not disrupt the computer network in any way.

Prohibitions

The use of the SHSD Network for illegal, inappropriate or unethical purposes by students is prohibited. More specifically:

1. Use of the SHSD Network to facilitate illegal activity is prohibited.
2. Use of the SHSD Network for commercial or for-profit purposes is prohibited.
3. Use of the SHSD Network for non-school purposes is prohibited.
4. Uses of the SHSD Network for product advertisement or political lobbying is prohibited.
5. Malicious use of the SHSD Network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer or system is prohibited.
6. Hate mail, harassment, discriminatory remarks, and other antisocial communications on the SHSD Network are prohibited.
7. The illegal installation, distribution, reproduction or use of copyrighted software on District computers is prohibited.
8. Use of the SHSD Network to access obscene or pornographic material is prohibited.
9. Use of the SHSD Network to transmit material likely to be offensive or objectionable to recipients is prohibited.
10. Use of the SHSD Network to intentionally obtain or modify files, passwords or data belonging to other users is prohibited.
11. Use of the SHSD Network to misrepresent other users on the SHSD Network is prohibited.
12. Use of SHSD technology or the SHSD Network for fraudulent copying, communications or modification of materials in violation of law is prohibited and will be referred to appropriate authorities.
13. Loading or use of unauthorized games, programs, files or other electronic media is prohibited.
14. The SHSD Network shall not be used to disrupt the work of others; and the hardware or software of other users shall not be destroyed, modified or abused in any way.
15. Use of the SHSD Network which results in any copyright violation is prohibited.
16. Never use another person's password to gain access to the SHSD Network.

Security

Security on any computer system is a high priority because there are so many users. If any SHSD Network user identifies a security problem, he/she must notify the system administrator or a teacher at once without discussing it or showing it to another user. The user must not use another individual's SHSD Network account. Any user identified as a security risk will be denied access to the SHSD Network.

Consequences

An SHSD Network user shall be responsible for damages to the equipment, systems or software resulting from deliberate or willful acts.

Failure to follow the procedures and prohibitions listed above may result in the loss of the right to access the SHSD Network. Other appropriate disciplinary procedures may take place, as needed, for students.

Illegal use of the SHSD Network, intentional deletion or damage to files of data belonging to others; copyright violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.

Limitation of Liability

SHSD makes no warranties of any kind, whether express or implied, for the service it is providing. SHSD will not be responsible for any problems suffered while on the Internet. These problems include but are not limited to loss of data as a result of delays or otherwise, non-deliveries, mis-deliveries, or service interruptions caused by the Internet or users which include errors or omissions. Use of any information obtained through the Internet is at the user's own risk. SHSD will not accept any responsibility for the accuracy of information obtained through the Internet.

Policy Administration

SHSD has implemented an electronic method for tracking student acceptance of this and other related policies. Failure to accept the policy will prevent the user from accessing network resources.

CIPA Definitions of Terms

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, and actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Student Acceptable Use Policy for Steelton-Highspire School District (CIPA Compliance): Computer Use
Adopted: 01/31/2009
Amended:
Reviewed without Amendment:
Steelton-Highspire School District
250 Reynders Avenue
Steelton, PA 17113