SHERMAN INDEPENDENT SCHOOL DISTRICT
STUDENT GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

These guidelines are provided so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CDROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations

a. Student use of computers, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a staff member.

b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center (library) of each campus as well as posted on the District's Web site (www.shermanisd.net).

c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

a. Using the network for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.

b. Using the network for financial or commercial gain, advertising, or political lobbying.

c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Bypassing internet filtering is strictly prohibited as is use or possession of hacking software.

e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
f. Intentionally wasting finite resources, i.e., online time, real-time music.

g. Gaining unauthorized access anywhere on the network.

h. Revealing the home address or phone number of one's self or another person.

i. Invading the privacy of other individuals.

j. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

k. Coaching, helping, observing, or joining any unauthorized activity on the network.

l. Forwarding/distributing e-mail messages without permission from the author.

m. Posting anonymous messages or unlawful information on the system.

n. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, or slanderous.

o. Falsifying permission, authorization, or identification documents.

p. Obtain copies of or modify files, data, or passwords belonging to other users on the network.

q. Knowingly placing a computer virus on a computer or network.

3. Acceptable Use Guidelines - Sherman Independent School District Network
Network Resources and Services

a. General Guidelines

(1) Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2) Students are responsible for their ethical and educational use of the computer online services in the District.

(3) All policies and restrictions of the SISD network services must be followed.

(4) Access to the Sherman Independent School District network services is a privilege and not a right. Each student, and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to the SISD Network computer online services.

(5) The use of any SISD network service in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6) When placing, removing, or restricting access to specific databases or other SISD computer services, school officials will apply the same criteria of educational suitability used for other education resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District Student Code of Conduct booklet.

(9) Parents concerned with the SISD computer network at their child's school should refer to the EFA(LOCAL): *Instructional Resources: Instructional Material Selection and Adoption* policy and follow the stated procedure.

(10) Any parent wishing to restrict their children's access to any SISD computer online services will provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.

b. Network Etiquette

(1) Be polite.

(2) Use appropriate language.

(3) Do not reveal personal data (home address, phone number, phone numbers of other people).

(4) Remember that other users of the SISD network services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

c. E-mail

(1) E-mail should be used for educational or administrative purposes only.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the SISD computer online services by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all contents are property of the District.

d. Consequences

The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

Noncompliance with the guidelines published here in the Student Code of Conduct and in Board policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequences of the Student Code of Conduct. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District. Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.
The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Open Records Act; proper authorities will be given access to their content.

THE SIGNATURE SHEET FOR THIS IS INCLUDED IN THE HANDBOOK AND WILL ALSO SERVE AS THE PERMISSION FORM FOR STUDENT INFORMATION TO BE INCLUDED ON THE SISD WEBSITE AND VIDEO CONFERENCING SYSTEMS. IT ALSO INCLUDES PERMISSION FOR ART REPRODUCTION.