

APPENDIX B

Southwest School Network / Internet Use Agreement (For All Personnel)

It is the responsibility of the administration to control access to data stored in the district's computer-based systems to maintain confidentiality where necessary, maintain integrity over the data and protect all computers and peripheral devices against unauthorized use. Only "authorized users" are given access to the district's computer-based systems. An authorized user is an employee who has the need to create or obtain data and has been authorized by a Supervisor. You have been identified as an authorized user. As an authorized user, you have certain responsibilities outlined as follows:

- Maintain confidentiality over your password
- Sign or log off your workstation when not in use or when workstation is unattended. As an authorized user, you are accountable for any actions performed under your password; therefore, it is more critical that you log off when leaving the workstation you are signed on to.
- Use of the computer network must be in support of education and research and consistent with the education objectives of SW Schools.
- Use of the computer network for illegal, inappropriate or unethical purposes by staff is prohibited. The determination as to whether a use is appropriate lies solely within the discretion of the SW Schools district.

More specifically, the following uses are prohibited:

- Use of the network to facilitate illegal activity
- Use of the network for non-school or non-work related activities. For example, visiting sites such as (*but not limited to*):
 - Any Message Boards, Blogs and or Chat Rooms
 - Youtube or other such Streaming Video sites
 - MySpace and or FaceBook type sites
 - Any Shopping website not being used for business purposes (Ebay, Target, Wal-Mart, Craigslist etc.)
- Use of the network for product advertisement, political lobbying, commercial or for-profit purposes
- Use of the network for hate mail, vulgar mail, discriminatory remarks and offensive or inflammatory communication. This includes chat rooms, web postings, Blogs, and e-mail.
- Use of the network to access or obtain obscene, sexually explicit or pornographic material to include the improper downloading of explicit music or word lyrics for reproduction, or distribution.
- Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials and the downloading of unauthorized games, program files, electronic media (music or video) or other non-district registered software
- Quoting personal communications in a public forum without the original author's prior consent

- Use of the network to intentionally obtain or modify files, passwords and data belonging to other users
- Impersonation of another user, anonymity and pseudonyms
- Vandalizing computer resources or electronic information services in any form. Vandalism includes uploading, downloading, or creating computer viruses and / or any malicious attempt to harm or destroy District equipment, electronic information services or the data of another user
- Use of the internet to access personal email during business hours for non-school work purposes

User accounts are property of the SW Schools district and staff should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the school computer network or stored in his/her directories. The school's computer network operator's and other authorized personnel may, at any time, review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted.

Any employee suspecting that computer security has been compromised is to report such information to the Administration immediately. The District reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity if this activity is discovered. Intentional misuse of data and / or computers can result in disciplinary action and possible termination. This policy applies to all:

- Computer data created or maintained within the mainframe computers systems.
- Computer data created or maintained within a district-wide mini-computer system.
- Data stored on file servers and workstations within the district.
- District data stored outside data processing services.

By signing below, you acknowledge that you have received a copy of this notice, that you understand the responsibilities of authorized users, and further understand that intentional misuse of data and / or computers can result in disciplinary action and possible termination of employment.

Employee Signature

Date

Print Full Name