SOUTHERN OKLAHOMA
TECHNOLOGY CENTER: DISTRICT POLICY BJ

INTERNET ACCESS, INTERNET SAFETY, AND ACCEPTABLE USE POLICY

PURPOSE: The purpose of this policy is to establish a set of guidelines and expectations that will enhance learning at SOTC while protecting employees, students, and partners from illegal or damaging actions by individuals either knowingly or unknowingly. Inappropriate use of technology exposes the District to many risks including viruses, compromised data, and other legal liability.

SCOPE: This policy applies to employees, students, partners, contractors or any other guests who access District resources using District owned or personal equipment.

I. **Acceptable Use** - The use of District resources must be in support of education or research and consistent with the educational objectives of Southern Oklahoma Technology Center. Transmission of any material in violation of U.S. or state law is prohibited. This includes, but is not limited to: copyright material, threatening or obscene material, material protected by trade secret, or other confidential information. Use for commercial activities, product advertisements, religious promotion, or political lobbying is also prohibited.

II. **Intellectual Property** - All "Intellectual Property", meaning databases, audio visual material, electronic circuitry, computer software, computer files, communications, information, inventions, or discoveries, generated through any activity associated with the District will be considered sole property of the District.

III. **General Use** – Employees, students, partners, contractors or guests are responsible for exercising good judgment regarding the use of the District's technology resources. The following activities are, in general, prohibited. While the list is not exhaustive, it is an attempt to provide a framework for activities which fall into the category of unacceptable use.

a. Introduction of malware or malicious software onto District resources is prohibited.
b. Port scanning or security scanning is expressly prohibited.
c. Executing any form of network monitoring which intercepts data not intended for the recipient is prohibited unless this activity is part of an employee's normal job/duty.
d. Revealing your password to others or allowing others to use your account is prohibited.
e. Circumventing user authentication or security of any host, network or account is prohibited.

Adopted: 7-1-98
Revised: 3-14-03
10-10-08
4-12-12
8-10-12

f. Bypassing or attempted bypassing of internet filters or other monitoring software is prohibited.
g. Using any program, script, or command with the intent to interfere with or disable a user's session is prohibited.
h. Sending unsolicited email messages, including the sending of "spam" or other advertising material to individuals who did not request such material is prohibited.
i. Posting non-business related messages to large numbers of individuals, including forwarding of chain letters or other "inspirational" type messages is prohibited.
j. Storing large amounts of personal photos, music files or other data on District owned servers or computers is prohibited.

IV. Social Networks (District or Professional Use) – When participating in a social networking site or blog in a professional capacity you **must** have the approval of the Superintendent to do so.

a. Do not post confidential or proprietary information about the District, its students, alumni, or employees on social networking sites or blogs.
b. Never pretend to be someone else and post information about the District.
c. Any information shared via social networking sites or blogs regarding the business of the District whether using personal or District equipment is considered public record and must be retained according to state and local laws.
d. Thoroughly check spelling and grammar before you post.
e. Be aware that blogs and social networking sites by their very nature are not private. Internet search engines can find information years after it was originally posted. Comments can be forwarded or copied even if you delete a post.

V. Social Networks (Personal Use) – The personal use of social networking sites or blogs creates the risk of affecting your professional career. To that end, it is vital that you conduct yourself in a way that does not adversely affect your position with the District.

a. Employees are prohibited from knowingly "friending" or communicating with current students on their personal social networking account. This does not include "professional" social networking accounts that may be created by the District Marketing Coordinator specifically for student/stake holder communication.
b. Posting of information or photographs that may be considered defamatory, libelous, obscene, or in violation of District policy, regulation or FERPA may result in professional repercussions.
c. You do not have control of what others may post on social networking sites; therefore, be aware that your conduct in your private life may affect your professional life.

Adopted: 7-1-98
Revised: 3-14-03
10-10-08
4-12-12
8-10-12

d. During the work day (unless on leave), including lunches or breaks, employees should refrain from participating in social networking sites that are personal in nature. Such activities leave time-stamps and could be misinterpreted by others.

VI. Harassment/Cyber-Bullying - With respect to electronic communications, students are specifically prohibited from bullying, harassing, threatening, or intimidating other students, employees, patrons, and guests regardless of where the electronic communication originated. Students may be suspended, transferred, expelled or face other disciplinary/legal action if found to be in violation. Harassment or bullying should be reported to an instructor or an administrator.

VII. Warranty - Southern Oklahoma Technology Center makes no warranties of any kind. The District is not responsible for any damages resulting from loss of data, delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the District's technology resources is at your own risk.

VIII. Privacy – While the District desires to provide a reasonable level of privacy, users should be aware that data or communications transmitted or stored using District resources is considered property of the District and may be accessed at any time without notification. For security and network maintenance purposes, authorized individuals within the District may monitor equipment, systems, and network traffic at any time.

IX. Children's Internet Protection Act (CIPA): Southern Oklahoma Technology Center has adopted *BARACUDA INTERNET SECURITY* as the technology protection measure (Internet Filtering Software). BARACUDA protects against access by adults and minors to visual depictions that are obscene, or with respect to use of computers with internet access by minors – harmful to minors.

Our Internet Acceptable Use Policy addresses the following as required by CIPA

a. Access by minors to inappropriate matter on the internet
b. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication.
c. Unauthorized access including so called "hacking," and other unlawful activities by minors online.
d. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
e. Measures designed to restrict minors' access to materials deemed harmful to minors.

X. Copyright Material – Students are prohibited from installing, copying, or downloading any copyrighted material or software on District's computer hardware. Employees are

prohibited from installing, copying, or downloading any copyrighted material or software on District's computer hardware without the express written consent of the copyright holder and the approval of the appropriate administrator or system operator.

XI. **Exceptions – General Use b., c.** These provisions are subject to the following exceptions: (a) port scanning, network monitoring as required as part of a student learning or demonstration within the confines of the lab environment and (b) the instructor isolates the teaching lab/network from the network in use by staff and other students or guests. (c) The instructor will notify the Information Technology Department of the demonstration or activity before it takes place. **Social Networks (Personal Use) a.** This provision is subject to the following exceptions: (a) communication with relatives and (b) if an emergency situation requires such communication, in which case the employee should notify his/her supervisor of the contact as soon as possible.

GLOSSARY:

Cyber-Bullying- is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as *Facebook* and *Twitter* to harass, threaten or intimidate someone. The *National Crime Prevention Council* defines cyber-bullying as "the process of using the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person."

Social Network Sites- We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.

Adopted: 7-1-98
Revised: 3-14-03
10-10-08
4-12-12
8-10-12