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 SouthernTech 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 the 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 that 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 that 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.
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.

Policy

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. District employees are expected to serve as positive ambassadors for our schools and remember they are role models to students in this community. Because readers of social media may view the employee as a representative of the District, they are required to observe the following rules when referring to the district, its students, programs, activities, employees, volunteers and communities on social media;

a. Do not post confidential or proprietary information about the District, its students, alumni, or employees on social networking sites or blogs. District employees may not disclose information on any social media network that is confidential or proprietary to the district, its students or employees or that is protected by data privacy laws such as FERPA. Posting images on any social media network of co-workers without the co-worker's consent is prohibited. Information or images of students may NOT be posted on any social media network without written consent.
b. Never pretend to be someone else and post information about the District. Employees may not act or purport to act as a spokesperson for the District or post comments as a representative of the District, except as authorized by the superintendent or the superintendent's designee. District employees must make clear that any views expressed are the employee's alone and do not necessarily reflect the views of 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.
f. An employee's use of any social media and an employee's postings, displays, or communications on any social media network must comply with all state and federal laws and any applicable district policies.
g. District employees will exercise discretion and maintain professionalism when communicating with students or groups of students via school-approved platforms or wireless telecommunication devices. Employees will limit communication with students to matters concerning a student's education, or extracurricular activities for which the staff member has responsibilities.
h. District's name/logo may not be used on any social media network without permission from the Superintendent, or designee. Nonpublic images of the District premises and property, including floor plans, may not be posted or shared.

Policy

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. District employees should be aware that persons classified as "friends" or persons who can access a personal social networking site may have the ability to download and share the employee's information and photographs with others. Employees are strongly encouraged to set and maintain social networking privacy settings at the most restrictive level.
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.
e. District employees are personally responsible for all comments/information they publish online. Respect and professionalism should be maintained in all communication – by word, image or other means. Employees shall not use obscene, profane or vulgar language on any social media network or engage in communications or conduct that is harassing, threatening, bullying, libelous, or defamatory or that discusses or encourages any illegal activity or the inappropriate use of alcohol, use of illegal drugs, sexual behavior, sexual harassment, or bullying.

VI. **Generative Artificial Intelligence (AI) Chatbots – Staff –** The use of generative AI chatbots will largely be allowed while performing work for the District. No proprietary District data may be submitted (copied, typed, etc.) to these platforms. Employees wishing to use generative AI chatbots should discuss the parameters of their use with their director/supervisor. Directors/supervisors may verbally approve, deny, or modify those parameters as best meet company policy, legal requirements, or other business needs.

VII. **Generative Artificial Intelligence (AI) Chatbots – Student** – The use of generative AI chatbots will be allowed with limitations while performing school work for the District. However, district-provided email addresses, credentials, or phone numbers cannot be used to create an account with these technologies. No proprietary District data may be submitted (copied, typed, etc.) to these platforms. Students wishing to use generative AI chatbots should discuss the parameters of their use with their instructor. Instructors may deny or modify those parameters as best meet company policy, legal requirements, or other business needs. See Student Handbook.

VIII. **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.

IX. **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.

X. **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.

XI. **Children's Internet Protection Act (CIPA):** Southern Oklahoma Technology Center has adopted CISCO MERAKI WEB FILTER AND FIREWALL as the technology protection measure (Internet Filtering Software). CISCO MERAKI 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.

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

XIII. **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.

Policy

XIV. Consequences for Violations of Social Media/Network Policy: Reports of a violation of this policy may result in an investigation of the user's posts, files, internet usage, or other electronic/digital media. The investigation and its scope will be reasonable, and calculated to disclose the existence and nature of the alleged violation. If warranted, consequences will be determined in accordance state and federal laws, considering the type of violation, past history, and level of the user.

Consequences may include, but are not limited to the following: 1) Loss of internet access (while on school property) and/or network access, for a determined amount of time according to the offense; or 2) Disciplinary action that may include a recommendation for dismissal or non-reemployment.

Policy

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.

Social media – refers to any user generated content sites generally available to the public or consumers that include, but are not limited to sites like Facebook, Flickr, YouTube, Twitter, Instagram, Snapchat, Google apps, Skype, Wikis, social networks, podcasts, forums, blogs, and other content sharing sites.

Generative Artificial Intelligence (AI) - artificial intelligence capable of generating text, images, or other media, using generative models. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.

Chatbot – A chatbot system uses conversational artificial intelligence (AI) technology to simulate a discussion (or a chat) with a user in natural language via messaging applications, websites, mobile apps or the telephone. It uses rule-based language applications to perform live chat functions in response to real-time user interactions.

Policy

Adopted: 7-1-98
Revised: 10-11-01
3-14-03
10-10-08
4-12-12
8-10-12
9-12-19
12-14-23
7-11-24
2-26-26