SOUTHERN OKLAHOMA TECHNOLOGY CENTER

Internet Safety/Acceptable Use Policy - STUDENT

PURPOSE: The purpose of this policy is to establish a set of guidelines and expectations that will enhance learning at Southern Tech 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.

1. **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.
2. **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
3. **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.
    - Introduction of malware or malicious software onto District resources is prohibited. Port scanning or security scanning is expressly prohibited.
    - 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.
    - Revealing your password to others or allowing others to use your account is prohibited. Circumventing user authentication or security of any host, network or account is prohibited. Bypassing or attempted bypassing of internet filters or other monitoring software is prohibited. Using any program, script, or command with the intent to interfere with or disable a user's session is prohibited.
    - Sending unsolicited email messages, including the sending of "spam" or other advertising material to individuals who did not request such material is prohibited.
    - Posting non-business related messages to large numbers of individuals, including forwarding of chain letters or other "inspirational" type messages is prohibited.
    - Storing large amounts of personal photos, music files or other data on District owned servers or computers is prohibited.

4. **Internet Etiquette (Netiquette) - Social Networks, Blogs, Bulletin Boards, Forums, News groups, email, etc.** – Internet Etiquette or "Netiquette" is acceptable behavior in electronic communication. All students are expected to comply with the District's "Netiquette" guidelines as outlined below when participating in online discussions or activities. This list is not exhaustive and is meant to provide a framework for appropriate behavior.

    - **Don't Participate in Flame Wars.** *(A flame war is a heated argument between two individuals that results in those involved posting personal attacks on each other.)* It's okay to disagree or constructively criticize an idea, but never personally attack another person.
    - **Always review and edit your communication before submitting.** Check grammar and spelling. Remember that social media venues are very public and leave a digital footprint for all to see, including future employers. To protect yourself, please observe social media policy guidelines when referring to the district, its schools, students, programs, activities, employees, volunteers and communities on any social media networks.

- **Keep your communications as clear and concise as possible.** Acronyms (LOL, IMHO, TTYL, etc.) are not acceptable.

Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts**.** Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or it is under Creative Commons attribution.

- **Respect and protect personal privacy.** Do not share personal, family, or classmate information. (e-mail addresses, phone numbers, birth dates, etc.) Do not "tag" individuals in photos that have requested not to be identified.
- **Be informal, not sloppy.** Your colleagues may use commonly accepted abbreviations in e-mail, but when communicating with external customers, everyone should follow standard writing
- **Keep messages brief and to the point.** Just because your writing is grammatically correct does not mean that it has to be long.
- **Use sentence case.** USING ALL CAPITAL LETTERS LOOKS AS IF YOU'RE SHOUTING. Using
- all lowercase letters looks lazy.
- **Use the blind courtesy copy and courtesy copy appropriately.** Don't use BCC to keep others from seeing who you copied.
- **Be sparing with group e-mail.** Send group e-mail only when it's useful to every recipient. Use the "reply all" button only when compiling results requiring collective input.
- **Don't send chain letters, virus warnings, or junk mail.** Always check a reputable antivirus Web site or your IT department before sending out an alarm.
- **Don't post or respond to any of the "Make Money Fast" postings.** Most are illegal, and no one in Nigeria will deposit any money into your account!
- **Remember that your tone can't be heard online.** Electronic communication can't convey the nuances of verbal communication. In an attempt to infer tone of voice, some people use emoticons, but use them sparingly so that you don't appear unprofessional.
- **Use a signature that includes your contact information.** To ensure that people know who you are, include a signature that has your contact information. Avoid pictures or large text in signatures.
- **Don't use social media** during school time unless specific permission has been granted by the District.
- **Adhere to all state and federal laws and any applicable district policies when posting on social media**. Students will be held accountable for the content of their electronic communications in relation to school, staff and students that might harm or cause harm to another student or teacher, and/or causes a disruption to the normal operations at school. Illegal behavior is subject to punishment as appropriate and available. Students who engage in cyberbullying also risk civil and/or criminal charges and/or lawsuits that may be filed against them by victims or victim's families. The district will fully cooperate with law enforcement agencies in any and all investigations involving students, electronic devices and social media.

6. Harassment/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 communications originated.

7. 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.

8. 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.

Acceptable Use Policy - Student

I _____ (Please Print) understand and will abide by the above stated Acceptable Use Policy. I further understand that any violation of the regulations may result in disciplinary action, and/or appropriate legal action.

Signature:_____ Date: _____

PARENT OR GUARDIAN ***(Required for Internet Users Under the Age of 18)***

Parent or Guardians Name (Please Print): _____

Signature: _____ Date: _____