INTERNET ACCESS AND ACCEPTABLE USE POLICY

General: The Internet is an electronic highway connecting a multitude of computers throughout the world. Through the Internet, students and employees have access to electronic mail (e-mail), news, databases, library resources, and a wide variety of other information sources. District provides various opportunities for students and employees to use District's computers to access the Internet. Through the Internet, it is possible to access material which may contain illegal, defamatory, inaccurate, pornographic, and/or offensive content. Due to the nature of the Internet, District cannot guarantee that students and employees will not access such material. However, District is committed to enforcing a policy of Internet safety, teaching appropriate online behavior, and monitoring the Internet activities of its students and employees.

District makes no warranties of any kind, either express or implied, regarding the Internet access being provided. District shall not be responsible for any damages users suffer, including but not limited to loss of data resulting from delays or interruptions in service. Nor shall District be liable for the accuracy, nature, or quality of information stored on District's computer equipment or of information gathered through Internet access provided by District. However, the Administration shall develop, implement, and maintain regulations and forms to restrict the use of the District's computers and Internet access to legitimate and acceptable purposes and to regulate students' and employees' privilege of access and use.

Acceptable Uses: District's computers, equipment, and software are intended for administrative, educational, and research purposes only and shall be used only in accordance with Administrative Regulations. Acceptable uses of District's computers and the Internet are activities which support learning and teaching or which promote District's mission and goals.

Prohibited Uses: According to Administrative Regulations, District's computers and available Internet access (including e-mail) provided by District shall not be used:

a. To violate an individual's right to privacy;

b. To access materials, information, or files of another person or organization without permission;

c. To violate the copyright laws or software licensing agreements;

d. To spread computer viruses;

e. To deliberately attempt to vandalize, damage, disable, or disrupt District's property or the property of any other individual or organization;

f. To locate, receive, transmit, store, or print files or messages which are profane, obscene, or sexually explicit, or which use language that is offensive or degrading to others;

g. To distribute religious materials;

h. To campaign for or against any political candidate or ballot proposition or for political lobbying, except as authorized by law;

i. For any commercial purpose unless authorized by the Administration or Board;

j. To engage in any illegal activity; or

k. To engage in cyberbullying at school or in the workplace.

Consequences for Misuse: The use of District's computers and the Internet access provided by District is a privilege, not a right. Any student or employee who inappropriately uses District's computers or the Internet may have the privilege of using the computers or the Internet denied, revoked, or suspended and may be subject to other disciplinary sanctions.

No Expectation of Privacy: No student or employee shall have any expectation of privacy in any computer usage, electronic mail being sent or received by District's computers or District-provided Internet access. District's system operators may access any electronic mail or computer usage and may delete any inappropriate material found, sent or received using the District's computers or District-provided Internet access. In addition, discipline may be imposed for improper usage.

Use of Software: 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.

Remote Internet-based Courses: District may allow for students to complete required course work through remote Internet-based courses in accordance with the rules, regulations, and/or guidelines adopted by the State Board of Education.

Internet-based Instruction: District may allow for students to complete required course work through Internet-based courses in accordance with rules, regulations, and/or guidelines adopted by the State Department of Education. Only regularly enrolled students of District shall qualify for such course credit and students enrolling in Internet courses shall be full-time students unless designated as suspended students or dropout students.

Education: District will educate all students who are granted access to the Internet regarding appropriate on-line behavior including: safety and security when using electronic mail, interacting with other individuals on social networking websites and in chat rooms, cyberbullying

awareness and response, and other forms of direct electronic communications, and the disclosure, use, or dissemination of personally identifiable information.

Web Filtering: All internet usage will be monitored and recorded to ensure compliance with the Children's Internet Protection Act ("CIPA"), as codified at 47 U.S.C. § 254. District shall provide filtered access to the Internet per standards pursuant to CIPA. Technology protection measures shall be in place that safeguards Internet access by all users to visual depictions that are obscene, related to child pornography, or other content that may be deemed harmful to minors. The Board delegates to the Administration the authority to determine matter that is inappropriate for minors.

District will enforce the operation of the technology protection measures on its computers with Internet access. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure during an audit, to enable access for bona fide research, or other lawful purposes.

Records Retention: District will retain its Internet Safety policy documentation according to the Record Retention and Archival of Electronic Mail Transmissions Policy - BM.

Employee and Student Use of Social Media: District recognizes the value and benefit of using electronic media to communicate digitally with students, families and fellow employees in an effort to engage stakeholders and enhance the learning experience. Whether or not an employee chooses to participate in online social networking or any other form of online publishing or discussion is his or her own decision. Free speech protects educators who want to participate in social media, but the laws and courts have ruled that schools can discipline students and employees if their speech, including online postings, interferes with the learning environment or causes a disruption to the normal operations at school, violates district policy or the laws of the State of Oklahoma.

District recognizes that the line between professional and personal relationships is blurred within a social media context. When employees choose to join or engage with students, families or fellow employees in a social media context that exists outside those approved by the district, they are advised to maintain their professionalism as district employees and take responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandatory reporting.

I. Employee Guidelines: The Superintendent, school principals and/or other members of District administration will annually remind all staff members the importance of maintaining proper decorum in the online/digital world, as well as in person. Employees must conduct themselves in ways that do not distract from or disrupt the educational process and complies will all state and federal laws and any applicable District policies. The reminders will give special emphasis to the following **prohibited behaviors:**

A. Improper socializing and improper private contact with students using social media sites, online networks, phones, technology and all communications.

B. Inappropriateness of posting items with sexual content.

C. Inappropriateness of posting items exhibiting or advocating use of drugs and alcohol or use of obscene, profane or vulgar language or engaging in communications or conduct that is harassing, threatening, bullying, libelous, or defamatory.

D. Monitoring and penalties for improper use of District computers and technology.

E. Intentional misinformation regarding District with purpose to damage and/or slander students, organizations, employees, schools, or administration. District employees must make clear that any views expressed are the employee's alone and do not necessarily reflect the views of the district.

F. Employees shall not engage in personal use of social media during contract hours unless online activity has been assigned to an employee and/or is related to an employee's work assignment. Use of an employee's personal social media account to discuss school business with parents and students is prohibited.

Per state law at 74 O.S. § 840-8.1, employees are discouraged from sharing content or comments containing the following when directed at a citizen of the State of Oklahoma:

A. Obscene sexual content or links to obscene sexual content;
B. Abusive behavior and bullying language or tone;
C. Conduct or encouragement or illegal activity; and
D. Disclosure of any information required to be maintained as confidential by law, regulation or internal policy.

"Social networking" or "social media" means interaction with external websites or services based upon participant contributions to the context. Types of social media include social and professional networks, blogs, micro blogs, video or photo sharing and social bookmarking; and "Comment" means a response to an article or social media content submitted by a commenter.

The Superintendent or designee will periodically conduct internet searches to see if employees have posted inappropriate materials/communications online. When violation of this policy is discovered, the material will be downloaded and promptly brought to the attention of the Superintendent or designee and District's legal counsel for review. Employees who engage in any of the above referenced prohibited behaviors are subject to disciplinary action, including possible dismissal from employment, for failure to follow district policy and/or state law.

A copy of this policy shall be distributed to each employee via e-mail. If information in violation of this policy and/or state law is posted on district social media, it will be immediately removed.

III. Student Guidelines:

A. 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.

B. Students should be aware that social posts must adhere to all state and federal laws and any applicable district policies. 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.

C. Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures.

D. 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.

E. Use of social media during the school day is prohibited unless specific permission has been granted by District.

IV. Consequences for Violations of Social Media 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, calculated to disclose the existence and nature of the alleged violation. If warranted, consequences will be determined in accordance with the collective bargaining agreements and 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:

A. Loss of internet access (while on school property) and/or network access, for a determined amount of time according to the offense.

B. Student offenses will include notifying the student's parent/guardian of an incident and possible disciplinary action appropriate to the severity of the offense.

C. Staff misuse may result in disciplinary action that may include a recommendation for dismissal or non-reemployment.

Adopted: September 14, 2020
Revised: