

INTERNET ACCESS, INTERNET SAFETY, 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. The District provides a wide variety of opportunities for students and employees to use the 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, the District cannot guarantee that students and employees will not access such material. However, the District is committed to enforcing a policy of Internet safety and monitoring the Internet activities of its students.

The District makes no warranties of any kind, either express or implied, regarding the Internet access being provided. The 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 the 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 the 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.

Internet Education for Students: The District is committed to educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Acceptable Uses: The 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 the District's computers and the Internet are activities which support learning and teaching or which promote the District's mission and goals.

Prohibited Uses: According to Administrative Regulations, the District's computers and the Internet access (including e-mail) provided by the 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 the 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; or
- j. To engage in any illegal activity.

Consequences for Misuse: The use of the District’s computers and the Internet access provided by the District is a privilege, not a right. Any student or employee who inappropriately uses the 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 electronic mail being sent or received by the District’s computers or District-provided Internet access. The District’s system operators may access any electronic mail and may delete any inappropriate material from any electronic mail sent or received using the District’s computers or District-provided Internet access.

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.

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.

Internet-based Instruction: The District may allow students to complete required course work through Internet-based courses in accordance with Oklahoma law, the rules, regulations, and/or guidelines adopted by the State Board of Education, and this policy. Students enrolled in Internet-based courses must participate in the Oklahoma School Testing Program. Test results for students enrolled in Internet-based courses must be disaggregated and reported.

The District authorizes any full-time student of the District to enroll in an approved Internet-based course offered by the District provided the course is determined to be appropriate for the student. The following criteria will be used to determine the appropriateness of Internet-based course work for a particular student:

- 1. A recommendation by the student’s teacher(s) that the student possesses the ability to work on his/her own;
- 2. The student has completed all prerequisites for the course as if it were offered through the District’s traditional class offerings;

3. The course will provide a means for the student to advance but is not a means for acceleration of a student's graduation date; and
4. The student is either suspended out-of-school or is in need of remediation.

All Internet-based courses must be approved by the Board prior to enrollment by students. The District shall use the following criteria to determine whether an Internet-based courses is approved for enrollment of students:

1. Teacher is certified to teach the course and trained in methodology and technical aspects of Internet-based instruction;
2. The course is aligned with Priority Academic Student Skills requirements;
3. A plan for monitoring and reporting student progress by the course instructor to the principal or principal's designee at least monthly with the final grade reported in time for inclusion on report cards/transcripts;
5. A course grading system that is compatible with the District's grading system and criteria;
6. Completion of the course must be within the school semester; and
7. The proposed Internet-based course is not duplicative of a course offered by the District.

Internet-based courses are not a means for students educated or enrolled elsewhere to enroll part-time in the District in order to take an Internet-based course. However, the District is authorized to enroll on a part-time basis for the purpose of utilizing Internet-base instruction students who have dropped out of school or who are or have been suspended. To be eligible, the student must have been enrolled in a public school in the state any time during the previous three (3) years.

Internet-based courses offered by a technology center and taught by a certified teacher and aligned with the appropriate Priority Academic Student Skills may be counted toward meeting the state graduation requirements with prior approval of the State Department of Education and the Board. Internet-based courses which contain integrated or embedded skills for which no Priority Academic Student Skills have been adopted may be approved by the Board if such courses incorporate national standards and are taught by certified teachers.

Remote Internet-based Courses: The 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 and this policy. However, students participating in remote Internet-based instruction will be required to provide their own equipment and Internet access and pay any associated fees, tuition, and/or expenses.

Web Filtering: The 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.

The District will enforce the operation of the technology protection measures on its computers with Internet access. An administration, 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: The District will retain its Internet Safety policy documentation according to the Record Retention and Archival of Electronic Mail Transmissions Policy - **BO**.