INTERNET AND TECHNOLOGY SAFETY

It is the policy of the district to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic or digital communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. §254(h)] and Oklahoma law [OKLA. STAT. tit. 70, § 11-202].

Definitions

The determination of what is "inappropriate" for minors shall be determined by the district. It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research and activity.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measures," "sexual act," and "sexual contact" shall be defined in accordance with the Children's Internet Protection Act, Oklahoma law, and any other applicable laws/regulations as appropriate and implemented by the district.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet Filters") shall be used to block or filter Internet (or other forms of electronic or digital communications) access to inappropriate information. Specifically, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

Any individual who uses the district's resources to access the Internet or engage in any electronic or digital communication is required to participate in the district's education efforts (undertaken pursuant to the Children's Internet Protection Act) and comply with the district's acceptable use policy.

Supervision and Monitoring

All employees are responsible for supervising and monitoring student use of the Internet in accordance with the district's technology policies, the Children's Internet Protection Act and Oklahoma law. The district's IT director shall establish and implement procedures regarding technology protection measures. No individual will be permitted to use the district's technology resources in a manner inconsistent with the district's policies.

Personal Safety

Employees and students shall not use the district's technology resources in any manner that jeopardizes personal safety. Students and employees must follow the district's technology policies, including the acceptable use policy which details the district's safe use standards.

Certification and Verification

The district shall provide certification, pursuant to the requirements of the Children's Internet Protection Act, to document the district's adoption and enforcement of its Internet and Technology Safety Policy, including the operation and enforcement of technology protection measures for all district computers with Internet access.

The district shall also obtain verification from any provider of digital or online library database resources that all the resources they provide to the district are in compliance with Oklahoma law and the district's Internet and Technology Safety Policy. If any provider of digital or online library resources fails to comply, the district shall withhold payment, pending verification of compliance. If any provider of digital or online library resources fails to timely verify compliance, the district shall consider the provider's act of noncompliance a breach of contract.

Reporting

No later than December 1 of each year, Oklahoma law provides that libraries shall submit to the Speaker of the Oklahoma House of Representatives and President Pro Tempore of the Oklahoma State Senate an aggregate written report on any issues related to provider compliance with Internet technology measures as required under Oklahoma law.

Employee Liability

Employees of the district shall not be exempt from prosecution for willful violations of state law prohibiting indecent exposure to obscene material or child pornography as provided under Oklahoma law [OKLA. STAT. tit. 21, § 1021].

Reference: 47 U.S.C. § 254(h); OKLA. STAT. tit. 70, § 11-202; OKLA. STAT. tit. 21, § 1021.

PROVIDER VERIFICATION

STATE OF _____)
)
COUNTY OF _____)

The undersigned, under penalty of perjury, certifies to Independent School District No. 8 of Tulsa County, Oklahoma (the "District") as follows:

1. I am a duly authorized representative of _____ (the "Provider").

2. The Provider has entered into a contract with the District to provide certain digital and online library database resources to the District.

3. I certify that the Provider agrees to abide by all terms of the District's policy on Internet and Technology Safety, and agrees that it is in compliance with Oklahoma law on digital or online library safety, as currently codified at Okla. Stat. tit. 70, § 11-202.

EXECUTED AND DELIVERED this _____ day of _____, 20___.

_____
Organization Name ("Provider")

By: _____
Name: _____
Title: _____

Subscribed and sworn to before me this ___ day of _____, 20__.

My Commission expires:

_____

_____
Notary Public

SUBSCRIBED AND SWORN to before me this _____ day of _____, 20___.

ACCEPTABLE USE OF INTERNET AND ELECTRONIC AND DIGITAL COMMUNICATIONS DEVICES

The forms of electronic and digital communications change rapidly. This policy addresses common existing forms of electronic and digital communication (email, texting, blogging, tweeting, posting, etc.) but is intended to cover any new form of electronic or digital communication which utilizes a computer, phone or other digital or electronic device.

As a part of the resources available to students and employees, the district provides Internet access at each school site and at its administrative offices. The district intends for this resource to be used for educational purposes and not to be used for conduct which is harmful. This policy outlines the district's expectations regarding Internet access. The ability to access the Internet while on school property is a privilege and not a right. Access cannot be granted until an individual has completed an "Internet Access Agreement" and access may be revoked at any time.

In addition to Internet access, the district also provides school employees, as needed, with a laptop for business use. This equipment is loaned to the employee for the remainder of the school year for the express purpose of increasing educational opportunities. The employee is required to return the laptop at the conclusion of the school year in the same condition the laptop was issued to the employee, minus normal wear and tear. In the event the laptop is damaged, lost or stolen, the employee agrees to reimburse the district in accordance with the laptop agreement.

Any individual using district resources to engage in electronic or digital communications has no expectation of privacy. Further, employees and students must be cognizant of the fact that electronic or digital communications which occur on private equipment are often permanently available and may be available to school administrators.

Employees and students are expected to use good judgment in all their electronic or digital communications - whether such activities occur on or off campus or whether the activity uses personal or district technology. Any electronic or digital communication which can be considered inappropriate, harassing, intimidating, threatening or bullying to an employee or student of the district - regardless of whether the activity uses district equipment or occurs during school/work hours - is strictly forbidden. Employees and students face the possibility of penalties, including student suspension and employee termination, for failing to abide by district policies when accessing and using electronic or digital communications.

The Internet provides users the ability to quickly access information on any topic - even topics which are considered harmful to minors. The district's IT department has attempted to filter this access in order to protect students from harmful content. In the event inappropriate material is inadvertently accessed, students should promptly report the site to their teacher so that other students can be protected. No individual is permitted to circumvent the district's privacy settings by accessing blocked content through alternate

methods. In the event an employee needs access to blocked content, he/she should make arrangements through the building principal or IT director.

Although the district's IT department has taken appropriate steps to block offensive material, users may unwittingly encounter offensive material. All users of the district's electronic resources are required to exercise personal responsibility for the material they access, send or display, and must not engage in electronic conduct which is prohibited by law or policy. If a student inadvertently accesses or receives offensive material, he/she should report the communication to the assigned teacher. If an employee accesses or receives offensive material, he/she should report the communication to the building principal or IT director. No individual is permitted to access, view or distribute materials which are inappropriate or create a hostile environment.

Internet Access - Terms and Conditions.

Acceptable Use - Students. Students agree to access material in furtherance of educational goals or for personal leisure and recreational use which does not otherwise violate this policy. No student may make an electronic or digital communication which disrupts the education environment - even if that communication is made outside of school or on personal equipment. Types of electronic or digital communications which can disrupt the education environment include, but are not limited to:

- Sexting
- Harassing, intimidating, threatening or bullying posts, tweets, blogs, images, texts, etc.
- Distributing pictures, recordings or information which is harmful or embarrassing

Students who engage in electronic or digital communications which disrupt the education environment are subject to disciplinary action, including suspension from school. Depending on the nature of the electronic or digital communication, students may also be subject to civil and criminal penalties.

Acceptable Use - Employees. Employees agree to access material in furtherance of educational goals, including research and professional development. Employees are also permitted to judiciously use the district's electronic resources for limited personal use, provided that the use is of no cost to the district, does not preempt business activity, impede productivity, or otherwise interfere with work responsibilities. Electronic or digital communications made using district owned equipment must be professional in nature and cannot be used for the exercise of the employee's free speech rights.

Any electronic or digital communication in which the employee can be identified as an employee of the district – regardless of whether the communication is made with district owned equipment or during work hours - must be a professional communication. Accordingly, if the individual is identifiable as a district employee, electronic or digital communications must not contain sexual, harassing, discriminatory or immoral content. Further, the communication cannot promote the use of tobacco, drugs, alcohol or be otherwise inconsistent with the district's objectives.

Employees are permitted to utilize electronic or digital communications with students provided the communication is available to all students of a specific group. For example, a teacher may create a dedicated site for all his/her students, or a coach may send a group text to all players on a team. In order to engage in any electronic or digital communications with students, an employee must make arrangements through the building

principal prior to the start of the year/season and must provide parents with a written plan for the electronic or digital communications. District employees are prohibited from engaging in private exchanges with students, and should only communicate with groups or in such a manner that the communication can be publicly viewed. Furthermore, employees are to refrain from engaging in electronic or digital communications which show an undue interest in select student(s), are of a personal nature, model inappropriate conduct, or are otherwise inconsistent with the district's mission and goals. Any employee who engages in unauthorized or inappropriate electronic or digital communication with students is acting outside the scope of his/her employment with the district.

Prohibited Use. Users specifically agree that they will not use the Internet to access material which is: threatening, indecent, lewd, obscene, or protected by trade secret. Users further agree that they will not use the district's electronic resources for commercial activity, charitable endeavors (without prior administrative approval), product advertisement or political lobbying.

Parental Consent. Parents must review this policy with their student and sign the consent form prior to a student being granted Internet access.

Privilege of Use. The district's electronic resources, including Internet access, is a privilege which can be revoked at any time for misuse. Prior to receiving Internet access, all users will be required to successfully complete an Internet training program administered by the district.

Internet Etiquette. All users are required to comply with generally accepted standards for electronic or digital communications, including:

a. Appropriate Language. Users must refrain from the use of abusive, discriminatory, vulgar, lewd or profane language in their electronic or digital communications.

b. Content. Users must refrain from the use of hostile, threatening, discriminatory, intimidating, or bullying content in their electronic or digital communications.

c. Safety. Students must not include personal contact information (name, address, phone number, address, banking numbers, etc.) in their electronic or digital communications. Students must never agree to meet with someone they met online and must report any electronic or digital communication which makes them uncomfortable to their teacher or principal.

d. Privacy. Users understand that the district has access to and can read all electronic or digital communications created and received with district resources. Users agree that they will not use district resources to create or receive any electronic or digital communications which they want to be private.

e. System Resources. Users agree to use the district's electronic resources carefully so as not to damage them or impede others' use of the district's resources. Users will not:

- install any hardware, software, program or app without approval from the IT department
- download large files during peak use hours
- disable security features

- create or run a program known or intended to be malicious
- stream music or video for personal entertainment

f. Intellectual Property and Copyrights. Users will respect others' works by giving proper credit and not plagiarizing, even if using websites designed for educational and classroom purposes (*See* www.copyright.gov/fls/fl102.html) Users agree to ask the media center director for assistance in citing sources as needed.

Limitation of Liability. The district makes no warranties of any kind, whether express or implied, for the services provided and is not responsible for any damages arising from use of the district's technology resources. The district is not responsible for the information obtained from the use of its electronic resources and is not responsible for any charges a user may incur while using its electronic resources.

Security. If a user notices a potential security problem, he/she should notify the IT director immediately but should not demonstrate the problem to others or attempt to identify potential security problems. Users are responsible for their individual account and should not allow others to use their account. Users should not share their access code or password with others. If a user believes his/her account has been compromised, he/she must notify the IT director immediately. Any attempt to log on to the district's electronic resources as another user or administrator, or to access restricted material, may result in the loss of access for the remainder of the school year or other disciplinary measures.

Vandalism. No user may harm or attempt to harm any of the district's electronic resources. This includes, but is not limited to, uploading or creating a virus or taking any action to disrupt, crash, disable, damage, or destroy any part of the district's electronic resources. Further, no user may use the district's electronic resources to hack vandalize another computer or system.

Inappropriate Material. Access to information shall not be restricted or denied solely because of the political, religious or philosophical content of the material. Access will be denied for material which is:

a. Obscene to minors, meaning (i) material which, taken as a whole, lacks serious literary, artistic, political or scientific value for minors and, (ii) when an average person, applying contemporary community standards, would find that the written material, taken as a whole, appeals to an obsessive interest in sex by minors.

b. Libelous, meaning a false and unprivileged statement about a specific individual which tends to harm the individual's reputation.

c. Vulgar, lewd or indecent, meaning material which, taken as a whole, an average person would deem improper for access by or distribution to minors because of sexual connotations or profane language.

d. Display or promotion of unlawful products or services, meaning material which advertises or advocates the use of products or services prohibited by law from being sold or provided to minors.

e. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, pregnancy, gender, gender expression or identity, national origin, religion, disability, veteran status, sexual orientation, age, or genetic information or advocates

illegal conduct or violence or discrimination toward any particular group of people. This includes racial and religious epithets, "slurs", insults and abuse.

f. Disruptive school operations, meaning material which, on the basis of past experience or based upon specific instances of actual or threatened disruptions relating to the information or material in question, is likely to cause a material and substantial disruption of the proper and orderly operation of school activities or school discipline.

Application and Enforceability. The terms and conditions set forth in this policy shall be deemed to be incorporated in their entirety in the Internet Access Agreement executed by each user. By executing the Internet Access Agreement, the user agrees to abide by the terms and conditions contained in this policy. The user acknowledges that any violation of this policy may result in access privileges being revoked and disciplinary action being taken. For students, this means any action permitted by the district's policy on student behavior. For employees, this means any action permitted by law, including termination of employment.

Education of Students Regarding Appropriate On-Line Behavior. In compliance with the Protecting Children in the 21st Century Act, Section 254(h)(5), the district provides education to minors about the appropriate use of the district's electronic resources, including interacting with others on social networking and chat sites, and cyber bullying. As a part of that education, guidelines on cyber bullying and internet safety for students are attached to this policy.

Cyber Bullying and Internet Safety Fact Sheet

People can be bullied in lots of ways, including through cyber bullying. Cyber bullying is when someone sends or posts things (words, pictures, recordings) that are mean, embarrassing or make people feel scared, embarrassed or uncomfortable. Even if they don't do this at school sometimes cyber bullying makes things at school hard. No student is allowed to disrupt school through cyber bullying.

Cyber bullies work in lots of ways, but here's some of their most common:

- Send or post mean messages
- Make up websites or accounts with stories, cartoons, pictures or "jokes" that are mean to others
- Take embarrassing pictures or recordings (without asking first)
- Send or post stuff to embarrass others
- Hack into other people's accounts or read their stuff
- Hack into other people's accounts and send or post their private stuff
- Pretend to be somebody else to get someone to give them private info
- Send threats

If you're a cyber bully knock it off! Ask your principal/counselor how you can make things right.

If someone is cyber bullying you, there's something you can do about it:

- Don't respond to and don't ignore a cyber bully. Instead, tell an adult you trust. If cyber bullying follows you to school, tell your teacher, counselor or principal.
- Even if what the bully does is embarrassing, don't delete it. Instead, get a copy so you can prove what happened.
- Have an adult help you contact a company representative (cell phone company, Yahoo, Facebook, Twitter, etc.) about blocking or removing the bad stuff.

You can't always stop people from being mean, but there are ways to help yourself:

- Don't give out your personal info in electronic or digital communications
- Don't tell anyone but your parents what your login name, password or PIN number is
- Don't post or send embarrassing pics or recordings (even on your own sites) - bullies love to copy your stuff

Suggestions for Parents:

- Help your child understand how permanent electronic or digital communications are
- Talk to your child about understanding, preventing and responding to cyber bullying
- Contact your student's school for help if you suspect your child is being cyber bullied – or if you suspect your child is engaging in cyber bullying

INTERNET ACCESS AGREEMENT
(STUDENTS)

STUDENT SECTION:

Student Full Name: _____

School Site: _____ Grade: _____

Home Address: _____

Home Phone No.: _____

I have received a copy of the policy titled *Acceptable Use of Internet and Electronic and Digital Communications Devices,* including the attachment regarding cyber bullying, and a copy of the *Student Handbook*. I have read and agree to abide by their provisions. I understand that any violation of the policy or handbook provisions may result in disciplinary action including, but not limited to, suspension and/or revocation of network privileges and suspension from school.

_____ _____

Student Signature Date

SPONSORING PARENT OR GUARDIAN SECTION (Required):

I have received a copy of the policy titled *Acceptable Use of Internet and Electronic and Digital Communications Devices*, including the attachment regarding cyber bullying, and a copy of the *Student Handbook*. I have read and discussed these provisions with my child. My child and I understand that any violation of the policy or handbook provisions may result in disciplinary action including, but not limited to, suspension and/or revocation of network privileges and suspension from school.

I understand that the school district has taken reasonable precautions to ensure that access to controversial material is limited to the extent possible, but I realize that it is not possible to guarantee that my child will never encounter objectionable material. I hereby release the school district from liability in the event that my child acquires inappropriate material through use of the district's technology resources, including the Internet.

I request that the district issue an account for my child and certify that the information contained on this form is correct.

_____ _____

Parent Signature Date

Student Access Agreement must be renewed each academic year.

INTERNET ACCESS AGREEMENT
(EMPLOYEES)

Employee Name: _____

Position: _____

School or Site: _____

Home Address: _____

Home Phone No.: _____

I have received a copy of the policy titled *Acceptable Use of Internet and Electronic and Digital Communications Devices*. I have read and agree to abide by its provisions. I understand that any violation of the use provisions may result in disciplinary action including suspension and/or revocation of network privileges as well as any discipline allowed by law including termination of employment.

_____ _____

Employee Signature Date

SPERRY PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology* Adopted: June 10, 2013 Revised: September 14, 2015; September 12, 2016; September 10, 2018; September 9, 2019

PERSONAL WIRELESS DEVICES AND ELECTRONIC ACCOUNTS

The district requires that all individuals devote their full attention to education while at school or during education activities. Accordingly, the district expects both employees and students to limit their use of personal wireless devices (including, but not limited to, hand-held mobile telephones) and personal electronic accounts at school or when engaged in district-related activities. Wireless devices include, but are not limited to, cell phones, laptops, cameras, GPS systems, any type of device capable of intercepting or recording a conversation, any type of device capable of providing visual surveillance or images, recorders, Google Glass, etc. Electronic accounts include, but are not limited to, accounts that allow digital communication such as email and social media accounts.

Google Glass and similar technology is prohibited on campus by all individuals at all times. Regardless of the type of technology used, no individual may make any type of surreptitious recording of others on district property. Additionally, no person may use any type of technology to remotely monitor, listen to, or view actions occurring at school or school activities. Personal wireless devices shall be turned off and out-of-sight in locations such as restrooms, locker rooms, changing rooms, etc. ("private areas"). The use of any audio/visual recording and camera features are strictly prohibited in private areas. Students who observe a violation of this provision shall immediately report this conduct to a teacher, coach, or the building principal. Employees who observe a violation of this provision shall immediately report this conduct to a supervisor, the building principal or other administrator.

<u>Students</u>

Students who possess a personal wireless device at school must keep that device turned off and out of sight during class time. No student will be permitted to access his/her personal wireless device during class time except with teacher permission due to an emergency. Students may use their personal wireless devices during breaks and lunch.

Students who violate this policy will have their personal wireless device confiscated until after a parent conference, and may lose the privileges of possessing such a device at school or school-related activities for the remainder of the school year. Students are also subject to other disciplinary action.

Students may not use any personal wireless device to:

- send or receive answers to test questions or otherwise engaged in cheating;
- record conversations or events during the school day, on school property or at school activities;

- threaten, harass, intimidate, or bully;
- take, possess, or distribute obscene or pornographic images or photos;
- engage in lewd communications;
- violate school policies, handbook provisions, or regulations.

Employees

Personal wireless devices may only be used during work time if the use of the device furthers the employee's performance of his/her professional responsibilities. No employee may use work time to engage in any personal electronic or digital communication, Internet activity, gaming, etc.

Employees will make reasonable efforts to use district resources rather than personal wireless devices or personal electronic accounts for electronic or digital communications with other employees, parents, and students and for tasks related to their employment. By using personal wireless devices or personal electronic accounts to communicate with other employees, parents, and students or to perform tasks related to their employment, employees acknowledge that they are creating records that may be subject to Oklahoma's laws related to Open Records (51 OKLA. STAT. § 24A.1 *et seq.*). Employees consent to retain and provide access to such communications or records to school district administration upon request. This consent survives any changes in the employment relationship.

Except for authorized transportation employees, no individual may use any personal wireless device while operating a district vehicle or while conducting school business in a personal vehicle.

Authorized transportation employees are permitted to utilize cell phones for business reasons to make or receive voice calls while operating a school bus or van, provided:

- the employee is using "hands free" technology to make the calls; or
- the employee has safely pulled the vehicle to the side of the road or is otherwise stopped and not impeding the flow of traffic.

Transportation employees are not permitted to text or otherwise use a personal wireless device while operating a district vehicle except as necessary to communicate with law enforcement officials, emergency services, or to and from the district's central dispatch transportation department.

Personal wireless devices may not be used to photograph or record conversations or events outside private areas without first obtaining consent to record from all parties. In the case of students, permission from the building principal must be obtained. Administrative approval for recordings of students will take into consideration whether prior approval has been granted from parents/guardians and whether the recording would identify a specific category of students such as special education students.

Personal wireless devices may only be shared with students for emergency use. No employee may use a personal wireless device to engage in conduct which is illegal or which could be construed as inappropriate conduct with a student or students. In the event an

employee receives an inappropriate electronic or digital communication from a student or parent, the communication must be promptly reported to the employee's supervisor.

The district fully acknowledges that personal wireless communications devices are the personal property of the employee. Unless an administrator has reasonable suspicion that an employee's personal equipment contains prohibited content, an administrator may not inspect an employee's personal equipment without the employee's express consent.

Warning: Possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images, photographs, or communications, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, and other modes of electronic or digital communication) may constitute a CRIME under state and/or federal law. Any person possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd or otherwise illegal images, photographs, or communications will be reported to law enforcement and/or other appropriate state or federal agencies, which may result in arrest, criminal prosecution, and inclusion on sexual offender registries.

SPERRY PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology* Adopted: June 10, 2013 September 9, 2013

SUPPLEMENTAL ONLINE COURSE PROCEDURES

Upon request, the district will provide supplemental learning opportunities using online technology in a non traditional classroom setting to students enrolled in the district. Supplemental online courses are an optional avenue of instruction for district enrolled students. All existing requirements related to student progression including retention, promotion, and grade assignment are the same for the district's online students as they are for students enrolled in traditional courses. The district shall ensure that students have the opportunity to advance through the supplemental online course at their own pace so long as the supplemental online course completion corresponds with the standard course completion schedule of the district or the student's Individualized Education Program (IEP) or 504 Plan.

Definition of Terms

A. "Supplemental online course"

An online program that allows students who are enrolled in a public school to supplement their education by enrolling part time in online courses that are educationally appropriate for the student, which are equal to the equivalent of classroom instruction time required for student attendance and participation by the district.

B. "Educationally appropriate"

For the purposes of supplemental online courses, educationally appropriate means any instruction that is not substantially a repeat of a course or portion of a course that the student has successfully completed, regardless of the grade of the student, and regardless of whether a course is similar or identical to the instruction that is currently offered in the school district. The determination of educationally appropriate will be made by the district.

Access to Supplemental Online Courses

Only public school students enrolled in the district will be granted access to supplemental online courses. The district provides enrolled students the opportunity to participate in supplemental online courses that comply with the standard curriculum of the district. Once a student has made a request to enroll in supplemental online course(s), the district will take necessary steps to determine the educational appropriateness of the request and to make online course(s) available to that student. Whether a requested online course is educationally appropriate for a student will be determined by the principal/curriculum director or his or her designee. Students may take supplemental online courses from online course providers selected and approved by the district that meet the criteria established by the Oklahoma State Board of Education (OSBE). The district shall not limit a student's access to supplemental online courses by either policy or application of internal or customary

procedures. However, students taking supplemental online courses from a remote location will be responsible for providing their own equipment and Internet access.

Funding

The district shall provide funding for an enrolled student's participation in online courses in an amount not to exceed the previous year's general fund per pupil expenditure. District students will be allowed to take up to the academic equivalent of five (5) hours of supplemental online instruction per day at no cost to the student. Students wishing to take more online course instruction may do so at their own cost. The district is not responsible to pay an online course provider for online course instruction expenses incurred by a student that exceed the pro-rated portion of the general fund per pupil expenditure for the student. The district will bear no responsibility for payment or collection of any outstanding funds or fees owed by a student to an online course provider.

School Day and Attendance Standards

Public school students enrolled at the district may take supplemental online courses from a location inside or outside of the school site location and may take supplemental online courses outside the normal school hours of operation. Students who elect to enroll in supplemental online courses, regardless of when or where taken, are still required to complete the equivalent number of hours of instruction as regularly enrolled students in the district and must satisfy the same attendance requirements of the district.

Students enrolled in supplemental online courses must meet all state mandated compulsory attendance requirements and are not exempt from state truancy laws. Attendance and participation in a supplemental online course shall be monitored in accordance with district policy and determined by documented student/teacher/course interaction that may include, but is not limited to, online chats, emails, and posting/submission of lessons. The student may be counted "in attendance" when the supplemental online course provider provides evidence of student/teacher/course interaction that demonstrates student progress toward learning objectives and demonstrates regular student engagement in course activity. Supplemental online course providers shall make available to students, parents, and the district, reports that reflect daily attendance and participation. Such attendance/participation reports shall be provided to parents and the district on a weekly basis via electronic format. The supplemental online course provider must provide evidence that the student is making appropriate progress weekly and such reports shall be sent to the designated resident district office via electronic format.

Student Eligibility, Admissions and Enrollment

Online supplemental courses that are educationally appropriate shall be offered to all qualifying district students who meet the following criteria:

A. The district offers individual academically approved and educationally appropriate online supplemental courses to students who are enrolled in the district. Students enrolled in supplemental online courses must meet all enrollment and eligibility criteria set by the district's residency policy, the Oklahoma State Board of Education Rules, and state law. Only students who are enrolled in the district for the current school year are eligible to enroll in supplemental online courses.

B. The admission process for students taking one or more supplemental online courses through the district shall be the same for students enrolled in traditional coursework.

C. The district shall allow for ongoing and continuous enrollment for supplemental online courses that are compliant with state law and all applicable State Board of Education rules. Students may have input as to the selection of supplemental online course providers but the final determination and selection of the providers is left to the discretion of the district.

D. Students enrolled in supplemental online courses shall have their progress monitored by the supplemental online course provider weekly. Progress reports shall be transmitted to the district's designated representative and the student's parent or guardian via electronic format. Such reports shall be reviewed by the district at least twice per month.

E. All public school districts in Oklahoma shall recognize course credit issued for courses authorized through the Supplemental Online Course Procedures.

F. Online course providers shall officially notify the district and parents in writing of the completion of each course the student takes within five (5) business days of completion. Course grades must be reported in the form of a percentage or in a manner consistent with district grading policies. The district shall use its established grading scale to convert the percentage to a letter grade or other notation consistent with district grading policies for transcript purposes.

G. District policies regarding grading scales and credits earned shall be applied to supplemental online courses under the same criteria as courses offered by the district. A grade assigned for course credit from a supplement online course shall be treated the same as any other course offered by the district.

H. Online course providers must report any change in a student's status (moving, dropping a course, etc.) immediately upon discovery or notification of the student's change in status.

Appeal Process

If a student's enrollment in a supplemental online course is denied based on a determination by the district that the course is not educationally appropriate, the parents or guardians of the student may appeal that determination to the district Superintendent. The district will notify the OSBE, Director of Instructional Technology, of any denial of a student's enrollment in online supplemental course(s), the reason for the denial, and any correspondence or information the district received in support of the student taking the online course.

Grace Period

A student may withdraw from a supplemental online course within fifteen (15) calendar days from the first day of a supplemental online course enrollment without academic penalty. A student who withdraws from any supplemental online course is still obligated to complete the equivalent number of classroom hours of education instruction that is required of students in the district in accordance with state law and district policy. The district shall not

be required to pay an online course provider for any student enrollment of less that fifteen (15) calendar days.

Extracurricular and Co-curricular Activities

Students enrolled in one or more supplemental online course may participate in extracurricular activities sponsored by the district in accordance with district eligibility rules and policies, the Oklahoma Secondary Schools Athletic Association (OSSAA) rules and regulations, and any other rules and regulations of a private association governing regulation of the interscholastic activities and contests of schools.

Student Assessments

Each student enrolled in one or more online course will participate in required state-level academic assessments administered pursuant to state law in the same manner as other regularly enrolled students within the state. The results of the assessments shall be released to the district and the online course provider. No student will be allowed to enroll in an online course without submission of a signed Education Student Assessment Results Release Form or FERPA waiver.

Special Education Students

The district shall provide supplementary aids and services, program modifications, supports for personnel and accommodations set forth in a student's IEP or Section 504 Plan to enable a student to take supplemental online courses that have been determined to be educationally appropriate for the student by the student's IEP or 504 team members. Provisions in the IEP for related services shall be the responsibility of the district where the student is enrolled in accordance with the Individuals with Disabilities Education Act (IDEA). Enrollment in a supplemental online course does not abdicate, modify or alter the district's legal obligation under the IDEA.

ACCEPTABLE USE OF FILE SHARING TECHNOLOGY

Employees and students may choose to use file sharing/storing technology (Google Docs, Ever Note, etc.) in connection with school learning or business. Individuals who choose to use such technology are required to follow all other district technology and acceptable use protocols, as well as adhere to the specific guidelines in this policy.

Individuals using file sharing/storing technology in connection with their association with the district are expressly prohibited from using the technology in a malicious manner or in any way which violates this or other district policies.

The district does not have agreements with any file sharing/storing technology providers. Individual users who utilize such technology in connection with the district specifically agree not to share or store files which contain:

- malware, viruses, worms, etc.
- information which is protected by FERPA or HIPAA
- confidential information such as home addresses, phone numbers, social security numbers, license numbers, dates of birth, and banking account numbers
- disciplinary or grievance information
- information about criminal investigations, including SRO records and notes
- safety sensitive information, including building layouts, evacuation routes, crisis response plans, etc.
- confidential or attorney client privileged information

Questions regarding whether information is acceptable for file sharing/storing technology should be directed to the Curriculum Director at 918-288-7213. Any individual who discovers that information has been improperly shared or stored is required to promptly notify the Curriculum Director of the violation. Individuals who violate this policy are subject to disciplinary action as outlined in district policies.

SPERRY PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology* Adopted: January 9, 2017

COMPUTER LOAN POLICY/AGREEMENT

Parental Responsibilities

Your son/daughter has been issued a ChromeBook computer to improve and personalize his/her education this year. It is essential that the following policies and rules be followed to ensure that your son/daughter receives the maximum benefit from the use of the computer and that the computer is used in a safe, efficient, and ethical manner.

- I will supervise my son/daughter's use of the computer at home.
- As a family, we will discuss appropriate places to use the computer to ensure its safety from dropping and damage.
- I will discuss our family's values and expectations regarding the use of the Internet and email at home and will supervise my son's/daughter's use of the computer to access the Internet and email accounts.
- I will not attempt to repair the computer, nor will I attempt to clean it with anything other than a soft, dry cloth.
- I will promptly report to the school any problem with the computer.
- I will not attempt to load or delete any software from the computer.
- I will make sure my son/daughter recharges the computer battery nightly.
- I understand that if my son/daughter comes to school without his/her computer I may be called to bring it to the school.
- If I am unable to bring the computer to school, my son/daughter may be required to complete an alternate assignment if the computer is being used in class and will still be responsible for completing the missing computer assignment.
- I agree to make sure the computer is returned to the school when requested and upon my son's/daughter's withdrawal from Sperry Public Schools.

I understand that if my son/daughter deliberately damages the computer or through negligence allows damage to the computer, beyond normal wear and tear, I will be liable for the following fines and may be responsible for replacement or repair of the computer, and my child will face additional consequences up to and including loss of computer use privileges or suspension.

1st Offense: Student will not be allowed to take the computer home for a period of two weeks, which would include two full weekends, and I will pay a fine of $25.00.

2nd Offense: Student will not be allowed to take the computer home for a period of nine weeks, and I will pay a fine of $50.00.

3rd Offense: Student will not be allowed to take the computer home for a period of one calendar year, and I will pay a fine of $100.00.

4th Offense: Student will not be allowed to take the computer home for the remainder of their enrollment at Sperry Public Schools.

NOTE: Student will, however, in each event be allowed to use a computer at school during the school day as needed to complete assignments, but may have Internet privileges limited or denied.

REPLACEMENT COSTS FOR EQUIPMENT:

- **$200.00 FOR CHROMEBOOK,**
- **$30.00 FOR PROTECTIVE CASE, AND**
- **$25.00 FOR CHARGER.**

Student Responsibilities

Your computer is an important learning instrument and is primarily for educational purposes. In order to receive permission to take your computer home, you must be willing to accept the following responsibilities:

- When using the computer at home, at school and anywhere else I may take it, I will follow all district policies and rules and abide by all local, state, and federal laws.
- I will treat the computer with care by not dropping it, getting it wet, leaving it outdoors, using it with food or drink nearby, or using it in horseplay.
- I will not loan the computer to anyone, not even my friends or siblings; it will stay in my possession at all times.
- I will not attempt to load or delete any software onto the computer.
- I will not remove programs or files from the computer.
- I will use my computer in safe locations as agreed to by my parents.
- I will not give personal information when using the computer.
- I will not use the computer to spread rumors or create conflict with other students.
- I will bring the computer to school fully charged every day.
- If I forget my computer, I understand I will be allowed to call home for someone to bring it to school.
- If I do not have my computer in class, I may be required to complete an alternate assignment if the computer is being used in class. I will still be responsible for completing the missed computer assignment.

- I agree that e-mail (or any other computer communication) should be used only for appropriate, legitimate, and responsible communication.

- I will keep all accounts and passwords assigned to me secure and will not share these with any other students.

- I will not attempt to clean or repair the computer.

- I will return the computer when requested and upon my withdrawal from Sperry Public Schools.

- I understand that if I violate any of these rules, I may lose the privilege to use the computer at home or even at school.

- I will return the computer in good condition and repair when requested and upon my withdrawal from Sperry Public Schools.

If I deliberately damage, or through negligence, allow damage to my computer, the following punishments will be enforced:

1st Offense: I will not be allowed to take the computer home for a period of two weeks, which would include two full weekends, and I will pay a fine of $25.00.

2nd Offense: I will not be allowed to take the computer home for a period of nine weeks, and I will pay a fine of $50.00.

3rd Offense: I will not be allowed to take the computer home for a period of one calendar year, and I will pay a fine of $100.00.

4th Offense: I will not be allowed to take the computer home for the remainder of my enrollment at Sperry Public Schools.

NOTE: I understand that I will, however, in each event be allowed to use a computer at school during the school day as needed to complete assignments, but may have Internet privileges limited or denied.

COMPUTER LOAN AGREEMENT

Student_____ Grade _____

Username _____ Home Phone _____

Home Address_____

Checkout Date _____ Scheduled Return Date _____

Item Description	Make and Model	Serial Number/ Item Number	Condition
	Make: Model:		

The above listed item (the "Equipment") is being loaned to the above named student and to the student's parents or legal guardians (collectively the "Borrower") and is new or in good working order. It is Borrower's responsibility to care for the Equipment and ensure that it is kept in a safe environment. This Equipment is, and at all times remains, the property of Independent School District No. 8 of Tulsa County, Oklahoma, a/k/a Sperry Public Schools (the "District") and is loaned to Borrower for educational purposes for the academic school year. Borrower may not deface or destroy this Equipment in any way. Inappropriate use of the Equipment or use in violation of the District's Acceptable Use Policy may result in the student losing his/her right to use this Equipment. The Equipment will be returned to the District when requested, at the end of the academic school year, or sooner, if the student withdraws from Sperry Public Schools prior to the end of the school year. The Equipment may be used by Borrower only for non-commercial purposes, in accordance with the District's Computer Loan Policy, Acceptable Use Policy, Student Handbook, and all applicable local, state, and federal laws, rules, and/or regulations.

Borrower may not install or use any software other than software owned or approved by the District and made available to Borrower in accordance with this Agreement. Borrower agrees not to copy or make any unauthorized use of or modifications of such software or to use such software in any way which violates the software license. Borrower agrees to indemnify the District for any claims arising from Borrower's misuse of the Equipment including claims alleging infringement of copyright or other intellectual property rights.

The District is not responsible for any computer or electronic viruses that may be transferred to or from Borrower's Equipment or data storage mediums and Borrower agrees to use Borrower's best efforts to ensure that the Equipment is not damaged or rendered inoperable by any such electronic virus while in Borrower's possession.

The Borrower shall be responsible for damages, resulting from negligence and/or intentional acts, to the Equipment and for loss or failure to return the Equipment. Borrower acknowledges and agrees that Borrower's use of the Equipment is a privilege and that by entering into this Agreement, Borrower acknowledges Borrower's responsibility to protect and safeguard the Equipment and to return the same in good condition and repair.

Parent Signature:_____ **Date:**_____

Print Name:_____ **Date:**_____

Student Signature:_____ **Date:**_____

SOCIAL MEDIA AND SOCIAL NETWORKING

The Sperry School District (the "district") recognizes the appropriate use of social media as a method for communicating ideas and information. The forms of electronic and digital communications change rapidly. Social media includes all means of communicating or posting information or content of any nature on the Internet, including but not limited to one's own or another's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat-room, whether or not associated or affiliated with the district, as well as any other form of electronic communication. This policy addresses common existing forms of electronic and digital communication (e.g., email, texting, blogging, tweeting, posting, etc.) but is intended to cover any existing or new form of electronic or digital communication which utilizes a computer, phone, tablet or other digital or electronic device.

Definitions

"Blog" means an online journal that contains entries or posts that consist of text, links, images, video or other media and is usually between 300-500 words.

"Comment" means a response to an article or social media content submitted by a commenter**.**

"Copyrights" protect the right of an author to control the reproduction and use of any creative expression that has been fixed in tangible form, such as literary works, graphic works, photographic works, audiovisual works, electronic works and musical works. It is illegal to reproduce and use copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.

"Hosted content" means text, pictures, audio, video or other information in digital form that is uploaded and resides in the social media account of the author of a social media disclosure. If an employee downloads content off of the Internet, and then uploads it to their own social media account, they are hosting that content. This distinction is important because it is generally illegal to host copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.

"Professional social media" is a work-related social media activity that is either school-based or non-school based.

"Cyberbullying" means the use of electronic information and communication devices, including, but not limited to email, instant messaging, text messaging, cellular telephone communications, Internet blogs, Internet chat rooms, Internet postings and defamatory websites.

"Social media account" means a personalized presence inside a social networking channel, initiated at will by an individual. YouTube, Twitter, Facebook, Instagram, SnapChat TikTok

and other social networking channels allow users to sign-up for their own social media account, which they can use to collaborate, interact and share content and status. When a user communicates through a social media account, their disclosures are attributed to their User Profile.

"Social media channels" means blogs, micro-blogs, wikis, social networks, social bookmarking services, user rating services and any other online collaboration, sharing or publishing platform, whether accessed through the web, a mobile device, text messaging, email or other existing or emerging communications platforms.

"Social media disclosures" are blog posts, blog comments, status updated, text message, posts via email, images, audio or video recordings, or any other information made available through a social media channel. Social media disclosures are the actual communications a user distributes through a social media channel, usually by means of their social media account.

"Social networking" or "social media" means interaction with external websites or services based upon participant contributions to the content. Types of social media include social and professional networks, blogs, micro blogs, video or photo sharing and social book marking.

Official Use of Social Media

The district is responsible for creating and maintaining its "official" online presence. Unless specifically authorized in writing by the Superintendent, no district employee may create an "official" district presence on or in any form of social media, now in existence, or created in the future, or represent themselves as a spokesperson or authorized representative of the district.

Professional Conduct

The district is committed to creating an environment in which all persons can interact in an atmosphere free of all forms of harassment, exploitation, or intimidation. Therefore, when communicating via social networks, employees are expected to act with honesty, integrity, and respect for the rights, privileges, privacy, and property of others. By doing so, employees will be abiding by applicable laws, school district policy and the core values of the district. The district prohibits abusive or offensive on-line behavior of employees at work or when engaged in work-related activities; likewise, district resources are not to be used in abusive or offensive ways. The district also discourages out-of-school on-line abusive or offensive behavior because of its potential to interfere with and disrupt work and student relationships.

Employees are responsible for the material they publish online as well as the messages they send via computers and wireless telecommunication devices. Any conduct that negatively reflects upon the district, consists of inappropriate behavior, or creates disruption on the part of an employee may expose that employee to disciplinary action up to and including termination. Inappropriate behavior is defined as any activity that harms students, compromises an employee's objectivity, undermines an employee's authority or ability to maintain discipline among students or work with or around students, is disruptive to the educational environment, or is illegal. Moreover, employees should not engage in personal social media during working hours.

Expectations

District employees are role models and must exemplify ethical behavior in their relationships with students, parents/guardians, patrons, and other staff members. Online activity, including personal online activity, is public and therefore a reflection on the district as an organization. Employees should exercise good judgment and common sense, maintain professionalism, and immediately address inappropriate behavior or activity discovered on district networks. Inappropriate behavior or activity should be immediately communicated to a direct supervisor. The following should inform and guide employee judgment and actions:

1. The line between professional and personal relationships can become blurred; therefore, district employees should always exercise discretion and maintain professionalism when communicating with students via computers or wireless telecommunication devices. Employees should limit this type of communication with students to matters concerning a student's education or extra-curricular activities for which the staff member has assigned responsibility. Excessive school-related messaging or other social media communication to an individual student should be avoided and an employee should only engage in social media communication with a student for a school-related purpose and with the consent of the employee's supervisor and the student's parent/guardian.

2. District employees are prohibited from engaging in private digital exchanges with students, and should only communicate with groups or in such a manner that the communication can be publicly viewed.

3. Photos of and videos featuring students should not be posted on social media without the informed consent of a parent/guardian. For personal protection, employees should never take a photo of an individual student.

4. Photos and videos of fellow employees should not be posted without their express permission.

5. Group student photos may be submitted to a principal or the superintendent for inclusion on official district accounts.

6. Students should not be cited, obviously referenced, or depicted in images without proper written approval of the student's parent/guardian; the confidential details of these individuals should never be disclosed.

7. Externally communicating any confidential information or information related to the district that is not intended for public dissemination is always forbidden and may be grounds for termination and legal action. Public information will be released through the superintendent or designee.

8. Copyright and fair use laws must be respected at all times. Trademarks such as logos, slogans, and digital content such as art, music, or photographs, may require

permission from the copyright owner. It is the responsibility of the employee to seek and obtain written permission for any such trademarked content.

9. District employees are discouraged from sharing content or comments containing the following when it is directed at a colleague, parent, student or citizen of the State of Oklahoma or the United States:

    a. Obscene and/or sexual content or links to obscene and/or sexual content;
    b. Abusive and bullying language or tone;
    c. Conduct or encouragement of illegal activity; and
    d. Disclosure of information which a school district and its employees are required to keep confidential by law, regulation or internal policy.

    Content or comments of the type listed above are especially concerning when directed at or exchanged with a student and may result in disciplinary action up to and including termination of employment and, possible referral to law enforcement or licensing and certification bodies.

10. The district is not interested in limiting an employee's ability to participate in personal social networks with a personal email address outside of the workplace. However, what is published on these sites should never be attributed to the district. Employees should make it clear that they are speaking for themselves. Furthermore, even if you do not mention the district, that information is readily ascertainable and could reflect poorly upon the employee and the district. Employees are encouraged to use common sense when making online comments, even if they intend for those to be purely personal in nature.

11. Employees are cautioned to be aware of their association with the district online social networks. If an employee identifies themselves as a district employee, the employee should ensure their profile, photographs, and related content are consistent with how the employee wishes to present themselves with colleagues, students, parents/guardians, and others.

Personal Use of Social Networking Sites (e.g., Facebook, TikTok, Twitter and Instagram, etc.)

1. Employees are personally responsible for all comments/information and hosted content published online. Employees should always be mindful that social media posts like tweets and status updates will be visible and public for an extended time.

2. By posting comments, having online conversations, etc. on social media sites, employees should remember that they are broadcasting to the world; accordingly, they should be aware that even with the strictest privacy settings, what one "says" online should be within the bounds of professional discretion. Comments expressed via social networking pages under the guise of a "private conversation" may still be shared by others in a more public domain.

3. Comments related to the district, its employees, and district events, should always meet the highest standards of professional discretion. Employees should always assume that every one of their postings is in the public domain.

4. Before posting personal photographs, employees should first consider how the posted images reflect on an employee's professionalism.

5. District employees are not permitted to solicit or accept "friend" requests from enrolled district students on any personal social media account. This includes student accounts and district employee personal accounts.

6. District employees are not permitted to encourage students enrolled in the district to create social media accounts of any kind.

7. All district employees who choose to utilize Facebook, TikTok, Twitter, Instagram or any other social media platform to provide classroom or extracurricular activity information to students and parents must create a "teacher" page, and posts must be exclusively about classroom or school activities.

Accountability

All staff are expected to serve as positive ambassadors for the district and appropriate role models for students. Failure to do so could put an employee in violation of district policy. This guidance and emphasis on personal judgment is provided because violation of district policies and procedures may result in disciplinary action up to and including termination of employment. All employees who have reason to believe that their on-line conduct has generated public or media attention are expected to immediately report their activity and the attention generated to their supervisor.

Staff-Student Relationships

Employees are prohibited from establishing personal relationships with students that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, but are not limited to: employees fraternizing or communicating with students as if employees and students were peers, e.g. writing personal letters or emails; "texting" students; calling students on a cell phone or allowing students to make personal calls to them unrelated to homework or class work; sending personal or inappropriate pictures to students; discussing or revealing to students personal matters about their private lives or inviting students to do the same (other than professional counseling by an assigned school counselor); and engaging in sexualized dialogue, whether in person, by phone, via the Internet or in writing.

Employees who post information on Facebook, Twitter or other similar platforms that include inappropriate personal information such as, but not limited to, provocative photographs, sexually explicit messages, use of alcohol, drugs or anything students are prohibited from doing must understand that if students, parents or other employees obtain access to such information, the employee's actions will be investigated by district officials; if warranted, an employee will be disciplined up to and including termination, depending on the severity of the offense, and may have their case forwarded to the Oklahoma State Department of Education for review and possible sanctions.

Distribution of Policy

This policy shall be distributed to all employees via the district's e-mail system at the beginning of each school year and at the time of hiring to all new employees hired after the start of the school year.

Reference: 74 O.S. §840-8.1

CYBERSECURITY

The District takes seriously the safety and security of its students and staff, which includes electronic security. Therefore, it is the policy of the District to have in place measures to prevent unauthorized access to its computer networks and to prevent the online theft, disclosure, use, or dissemination of personally-identifiable information stored on its computer networks (a "security incident").

Cybersecurity Protection Measures Generally

The Technology Director shall be responsible for the design and monitoring of measures to prevent and respond to unauthorized or unlawful access to or use of data on the District's computer networks ("preventative measures"). These measures shall include identifying network vulnerabilities, developing disaster recovery and business continuity plans, establishing clear procedures that comply with this policy, and educating all stakeholders and users on the importance of computer network security. Additionally, the storage of personally-identifiable information stored on District computer networks should be designed so that in the event of a data breach incident, the following data elements associated with the first name or first initial and last name of an individual are either encrypted or redacted: (a) social security number, (b) driver license number or state identification card issued in lieu of a driver license, or (c) financial account number, or credit card number, in combination with any required security code, access code, or password that would permit access to the financial account of the individual.

Security and Monitoring

The District will take reasonable efforts to maintain computer network security, whether threatened by security breach, human error, hardware malfunction, or otherwise. The Technology Director shall be responsible for securing and actively monitoring the District's computer network ("network") to identify, contain, mitigate, and report any security incident, which may include contracting with a third party for such services. However, any staff member who suspects or becomes aware of a security incident shall immediately notify the Technology Director.

The Technology Director shall also be responsible for designing, or having in place, adequate preventative measures, including perimeter and access controls, to regulate digital traffic between the District's computers and external entities. To the extent practicable, the electronic transmission of personally-identifiable information should be encrypted or redacted. Additionally, the Technology Director shall ensure the District's network and all District computer equipment are protected from malicious software attacks such as viruses, ransomware, spyware, and malware by commercial grade cybersecurity software and appropriate and regularly-updated software, including timely installation of necessary software patches.

The Technology Director shall annually report to the board of education regarding the adequacy of the District's preventative measures, including any security incidents that have occurred, the District's responses to those incidents, and subsequent improvements to network security. The Technology Director shall also conduct vulnerability assessments to monitor the efficacy of the District's preventative measures and make ongoing improvements or updates to security protocols, systems, hardware, and software as necessary.

The Technology Director shall also develop a disaster recovery or business continuity plan to be implemented in the case of a disaster or serious security incident which compromises the District's network and/or the data stored thereon. This plan shall include procedures for routinely backing-up District data to a secured, off-site location or onto appropriate backup media at a secure, off-site location. The District may contract with a third party for such services. At least annually, the Technology Director shall conduct contingency testing to ensure the speedy restoration of District systems and information in the event of a security incident or a disaster.

Response and Reporting

In the event of a security incident, the Technology Director shall immediately notify the Superintendent of Schools, and they, in consultation with the District's legal counsel, shall take such reasonable and appropriate steps as may be required, which may include notification to law enforcement and affected parties.. The Superintendent shall also notify the Board of Education of any security incidents as soon as practicable.

Education

The Technology Director is responsible for providing annual information technology training to District personnel who have access to sensitive and personally-identifiable information. This training will emphasize such employees' personal responsibility for protecting the District's network and personally-identifiable information. Additionally and on an ongoing basis, the Technology Director will provide guidance to all District employees on best practices to mitigate against the threats of a cyber-attack.

Reference: OKLA. STAT. tit. 74, § 3113.1; OKLA. STAT. tit. 24, §§ 161–166 ("Security Breach Notification Act"); 20 U.S.C. § 1232g, 34 C.F.R. Part 99 ("FERPA"); 47 U.S.C. § 254; 47 C.F.R. § 54.520 ("Children's Internet Protection Act"); 20 U.S.C. § 7131 ("Elementary and Secondary Education Act"); 15 U.S.C. § 7001