

## **INTERNET AND TECHNOLOGY SAFETY**

It is the policy of the technology center 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].

### Definition

The determination of what is "inappropriate" for minors shall be determined by the technology center. 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 technology center.

### 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 technology center's resources to access the Internet or engage in any electronic or digital communication is required to participate in the technology center'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 minor student's use of the Internet in accordance with the technology center's policies, the Children's Internet Protection Act, and Oklahoma law. The technology center's IT director shall establish and implement procedures regarding technology protection measures. No individual will be permitted to use the school's technology resources in a manner inconsistent with the technology center's policies.

### Personal Safety

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

### Certification and Verification

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

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



**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, , 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 technology center provides Internet access at each campus and at its administrative offices. The technology center intends for this resource to be used for educational purposes and not to be used for conduct which is harmful. This policy outlines the technology center's expectations regarding Internet access. The ability to access the Internet while on technology center 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.

Any individual using technology center 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 school technology. Any electronic or digital communication which can be considered inappropriate, harassing, intimidating, threatening or bullying to an employee or student of the technology center - regardless of whether the activity uses technology center equipment or occurs during school/work hours - is strictly forbidden. Employees and students face the possibility of penalties, including student suspension or dismissal and employee termination, for failing to abide by technology center 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 technology center'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 instructor so that other students can be protected. No individual is permitted to circumvent the technology center'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 campus director or IT director.

Although the technology center's IT department has taken appropriate steps to block offensive material, users may unwittingly encounter offensive material. All users of the technology center'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 instructor. If an employee accesses or receives offensive material, he/she should report the communication

to the campus director 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 or dismissal 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 technology center's electronic resources for limited personal use, provided that the use is of no cost to the technology center, does not preempt business activity, impede productivity, or otherwise interfere with work responsibilities. Electronic or digital communications made using technology center 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 technology center – regardless of whether the communication is made with technology center owned equipment or during work hours - must be a professional communication. Accordingly, if the individual is identifiable as a technology center 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 technology center's objectives.

**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 technology center's electronic resources for commercial activity, charitable endeavors (without prior administrative approval), product advertisement or political lobbying.

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

**Privilege of Use.** The technology center'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 technology center.

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.** Minor students must not include personal contact information (name, address, phone number, address, banking numbers, etc.) in their electronic or digital communications. Minor 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.
- d. **Privacy.** Users understand that the technology center has access to and can read all electronic or digital communications created and received with technology center resources. Users agree that they will not use technology center resources to create or receive any electronic or digital communications which they want to be private.
- e. **System Resources.** Users agree to use the technology center's electronic resources carefully so as not to damage them or impede others' use of the technology center'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](http://www.copyright.gov/fls/fl102.html)) Users agree to ask their instructor for assistance in citing sources as needed.

**Limitation of Liability.** The technology center 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 technology center's technology resources. The technology center 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 technology center'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 technology center'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 technology center's electronic resources. Further, no user may use the technology center'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 technology center'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 21<sup>st</sup> Century Act, Section 254(h)(5), the technology center provides education to minors about the appropriate use of the technology center'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.

Reference: 70 O.S. § 6-401