SECTION IV: STUDENTS POLICY 4295

STUDENT 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 may provide students with a Chromebook or other similar devices. This equipment is issued to the student for the remainder of the school year for the express purpose of increasing educational opportunities. The student may be required to return this device at the conclusion of the school year in the same condition it was issued to the student, minus normal wear and tear. In the event the device is damaged, lost or stolen, the student's parent or guardian agrees to reimburse the District in accordance with the fee schedule attached to the Electronic Device Agreement, unless a District device insurance policy was purchased. If a District policy is purchased, then rules pertaining to the insurance policy would apply.

Any individual using District resources to engage in electronic or digital communications has no expectation of privacy. Further, 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. In situations where a student has communicated intent to self-harm or harm others, the District will attempt to contact parents and/or law enforcement when these alerts are brought to our attention. However, District personnel do not monitor these devices 24 hours a day, 7 days a week nor do we expect District personnel to monitor school electronic or digital communications on non-school days, weekends, nights or holidays and cannot be liable for the actions of students.

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. Students face the possibility of penalties including student suspension 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. 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. Notwithstanding the foregoing, no student may photograph or make any audio or video recording of themselves or of any other person during the instructional day without permission from appropriate school official.

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:

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

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

3. 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.

4. 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.

5. 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

6. 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:

1. 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.

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

3. 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.

4. 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.

5. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, 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.

6. 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.

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 unless approved by the site administrator. 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 not otherwise prohibited 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.

It is the district's policy that 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.

Students may not use any personal wireless device to:

- send or receive answers to test questions or otherwise engage 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.

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.

Source: *Broken Arrow Board of Education policy adoption, August 10, 2015.*
Broken Arrow Board of Education policy revised, November 12, 2018.
Broken Arrow Board of Education policy revised, November 4, 2019.

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/Guardian Signature Date

Student Access Agreement must be renewed each academic year.

ELECTRONIC DEVICE AGREEMENT

Student Section

Student Full Name: _____

School Site: _____ Grade: _____

Home Address: _____

Phone No.: _____

Terms

The district has provided the student with a _____ for educational purposes for the current school year. The device's identifying information is:

Make / Model: _____

Serial No.: _____

The student's right of possession and use is limited to educational purposes and must comply with all District policies and procedures. The school district is the owner of the and is entitled to claim possession of the device at any time the administration deems appropriate. The student agrees to return the device on ____ or the student's last day of enrollment in the District, whichever is earlier.

The school district reserves the right to use tracking and other anti-theft software on the _____ to protect its ownership interests in the device.

If the _____ is stolen, the student/parent is responsible for filing a police report and notifying the technology director in writing within 48 hours of the theft. The student/parent must provide a copy of the police report to the technology director within 1 week of the theft. If this procedure is followed, the student/parent will not be financially responsible for the loss. If the _____ is lost or is not reported as outlined above, the student/parent will be financially responsible for the loss/theft.

Student/parent agree to be financially responsible for loss or damage to the device (except as noted above) in accordance with the following schedules:

Broken screen	$
Broken keyboard	$
Power adapter / cord	$
Battery	$
Re-image hard drive (due to improper use)	$
Case	$
Other	As determined by the District's IT department
Total loss of unit	$

Parent Section

I have read the foregoing agreement and agree to be bound by the terms of the agreement, including the financial terms outlined above. My student has permission to receive this equipment.

_____ _____

Parent/Guardian Signature Date