SECTION VI: BUSINESS, TECHNOLOGY & OPERATIONS POLICY 6110

INTERNET AND TECHNOLOGY SYSTEMS SAFETY AND APPROPRIATE USE

It is the policy of the Broken Arrow School District to:

1. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

2. Prevent unauthorized access and other unlawful online activity;

3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. 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. § 11-201].

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

To the extent practical, steps shall be taken to promote the safety and security of users of the Broken Arrow School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

1. Unauthorized access, including so-called "hacking", and other unlawful activities; and

2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

With respect to promoting the safety and security of minors, it shall be the responsibility of the Broken Arrow School District to educate minors about appropriate online behavior, including cyber bullying awareness and response and interacting with other individuals on social networking sites and in chat rooms. The Broken Arrow School District may implement this requirement in a number of different ways, including but not limited to:

1. Distribution of this policy to all students at the first of the year which contains such information;

2. Including such information in orientation for students at the beginning of each year in each computer class;

3. Talking to students about such matters each time an incident occurs that involves these matters; and

4. Any other manner deemed appropriate by the Superintendent or Board.

Supervision 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 Department 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.

It shall be the responsibility of all staff of the Broken Arrow School District to supervise and monitor usage of the online computer network and access to the Internet in accordance with the district's technology policies, the Children's Internet Protection Act, Oklahoma law. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or designated representatives.

Unacceptable uses of computer and electronic communications resources includes use that jeopardizes personal safety, use that involves illegal and prohibited activities, and use that threatens the security of the District's technology resources.

The Technology Department 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 Department shall conduct contingency testing to ensure the speedy restoration of District systems and information in the event of a security incident or a disaster.

Personal Safety

Employees and students shall not use the District's technology resources in any manner that jeopardizes or poses a threat to personal safety. The following directives are essential to ensuring personal safety:

1. Users shall not post personally identifiable information about themselves or others. For example, it is not permissible to put people's photographs on the web and identify them by name.

2. Student users shall not agree to meet or meet with someone they have met online, without parental approval.

3. Student users shall promptly disclose to their instructor or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

4. Users shall receive or transmit communications using only District-approved and District-managed communication systems. For example, users may not use free, web-based e-mail, messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the District's authorized supervisory personnel.

5. Users shall not attempt major repair of District-owned technology resources without the assistance of the District support mechanism. Major repair is defined as any repair or modification which has the potential to impact the District infrastructure, more than one workstation, disrupt business operations or requires the user to add or remove hardware. However, users are encouraged to perform troubleshooting and minor repairs in conjunction with the District technology support segment.

Illegal Activities

Engaging in illegal and prohibited activities involving use of the District's technology is prohibited. The emerging and fast-paced developments in technology make it impossible for the District to anticipate every potential use or misuse of its technology resources. Accordingly, users are instructed that the District's technology is not to be used for illegal activities. Among other things, users are expected to abide by the following:

1. Users shall not plagiarize works that are found on the Internet or any other electronic resource. Plagiarism is presenting the ideas or writings of others, as one's own.

2. Users shall respect the rights of copyright owners. Copyright infringement occurs when the user inappropriately reproduces a work that is protected by a copyright. Users shall not illegally copy protected works, or make copies of such works available. Users are responsible for observing any copyright or licensing agreement that may apply when downloading materials. Users may not download any material for which a fee or license agreement is required without the approval of appropriate District supervisory personnel. Users shall not install any software (including public domain software or freeware) which is not on the District's approved software list.

3. District staff will not support or maintain any computer operating system or application software that does not meet District standards.

4. Illegal installation of copyrighted software is prohibited. Illegal copying of software from any District computer, network, or program diskette is prohibited. Computer software and

data protected under copyright laws may not be downloaded or uploaded to a computer owned or leased by the District without the written consent of the copyright holder. Any software or data located on a computer or file server owned or leased by the District found to be in violation of copyright laws will be removed.

5. Users shall not attempt to gain unauthorized access or attempt to go beyond authorized access to District resources or to any other computer system. This includes attempting to log in through another person’s account or access another person’s files.

6. Users shall not make deliberate attempts to disrupt the District’s computer system or other portions of the technology resources or destroy data by spreading computer viruses or by any other means.

7. Users shall not congest the District’s technology resources or interfere with the work of others within or outside of the District when accessing the Internet, including the transmission or posting of messages that are intended or likely to result in the loss of the recipient’s work or systems.

8. Users shall not use the District’s technology resources to engage in any activities which interfere with the operation of the District or its educational programs or compromise the safety and security of the District’s technology resources.

Security of District’s Technology

The District spends substantial monies to provide students and staff with technology resources appropriate for the diverse educational and training interests associated with education objectives in a technology rich world. Users are required to adhere to the highest standards of use to avoid compromise or destruction of the District’s resources. Security with respect to the District’s technology resources requires adherence to the following:

1. Users shall access the Internet in a manner which does not compromise the security and integrity of the District’s technology resources, such as allowing intruders or viruses into the District’s technology resources. Users wishing to download any document, file or software from non-District sources must observe District policies and procedures for virus checking and system security.

2. Users are responsible for their individual logon passwords and e-mail account passwords and should take all reasonable precautions to prevent others from being able to use these passwords. Users shall not share e-mail passwords, provide e-mail access to an unauthorized user, or access another user’s e-mail without authorization.

3. A computer logged into the District wide area network or the internet should not be left unattended. Users are responsible for all transactions made under their User ID and Password.

4. Users must immediately notify the e-mail administrator if they identify a possible security problem.

5. Users are responsible for the appropriate storage and backup of their data.

6. The administration, faculty or staff of the District may request a system administrator to deny, revoke or suspend specific user accounts for violation of these policies or procedures.

Inappropriate Communications

Inappropriate communications are prohibited and can result in removal of access, or other disciplinary action. Users must adhere to the following directives:

1. Users shall not use, view, download, copy, send, post or access obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful information, communications, language, images, or video, or material that advocates illegal acts, violence, or discrimination towards others. Restrictions against inappropriate language, images or video apply to public messages, private messages, material posted on web pages, and files stored or created on the District's technology resource.

2. If a user mistakenly accesses inappropriate information, the user must immediately inform his/her teacher or the network supervisor of the location of that information.

3. Parent or guardians should instruct the student user if there is additional material that they think it would be inappropriate for their child to access. The District fully expects that student users will follow the instructions of their parents or guardians in this matter.

4. Users shall not post information that could cause damage or pose a danger of disruption to the operations of the technology resources or the District.

5. Users shall not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by another person to stop any activity which that person finds harassing, the user must stop immediately. Individuals who believe they are the victim of harassment should immediately contact their supervisor, campus administrator, or the Superintendent.

6. Users shall not knowingly or with reckless indifference post messages that are false or defame or libel any person or organization, or that infringe the privacy rights of others.

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.

Disciplinary Action

The use of District's technology resources is a privilege, not a right. Violation of District policies and procedures may result in cancellation of computer-use privileges and/or other disciplinary action up to and including termination of employment for employees and suspension from school for students. If Federal and/or State laws are violated, the offender is also subject to being reported to proper authorities for prosecution.

Reference: 47 U.S.C. § 254(h); OKLA. STAT. tit. 70. § 11-201; OKLA. STAT. tit. 21, § 1021.

Source: *Broken Arrow Board of Education policy adoption, July 13, 2009.*
Broken Arrow Board of Education policy revised, July 10, 2017.
Broken Arrow Board of Education policy revised, November 9, 2020.
Broken Arrow Board of Education policy revised, November 7, 2022.