INTERNET AND OTHER NETWORKS RESPONSIBLE USE AND SAFETY ~~ACCESS, INTERNET SAFETY, PERSONALLY OWNED DEVICES, AND USE OF ELECTRONIC RESOURCES~~

Oklahoma City Public Schools provides network and Internet access for educational purposes only. Users of the network not only agree to follow this policy, but also to take responsibility for appropriate and lawful use. All users should report any policy violations to an appropriate staff member. Throughout this policy, "district account" or "district password" refers to the user's single username and password used to login to computers, district email, and the district's student information system.

Inappropriate Use for All Users

In using the network and Internet, the following situations or activities are considered inappropriate use and constitute a violation of this policy, regardless of whether the individual engaging in such activities is a student, a school district employee, or any other individual:

- Sharing passwords, using another's account, or impersonating another user. Exceptions:
  - Students are allowed to share their passwords with their parents/guardians, teachers, or district technology department staff upon request.
  - Upon supervisor approval, district staff may share accounts (excluding the district account) to access systems that have technical or other limitations that hamper individual user accounts.
  - For troubleshooting purposes only, district technology department staff may access systems as another user. Such access will be documented.
- Using the network or Internet to:
  - Violate the law or encourage others to violate the law.
  - Gain or attempt to gain unauthorized access to data or systems.
  - Jeopardize the security of others' access or data.
  - Cause harm to others, including disrupting network access or capacity.
  - Invade others' privacy.
  - Sell or promote the use of any substance prohibited by district policy.
  - View or transmit material that is obscene, pornographic, child pornography, or harmful to minors.
  - Disrupt others' access or data.
  - Promote or conduct personal commercial activities or use district email to conduct personal business.
  - Promote a specific political entity.
- Cyberbullying is when one or more person(s) intentionally harm, harass, intimidate, or reject another person using technology. Cyberbullying will not be tolerated under any circumstances. This includes, but is not limited to, the following:
  - Sending mean, embarrassing, or threatening messages via e-mail, instant messaging (IM), text messages, or other network tools.
  - Stealing another person's login and password to send mean, embarrassing, or threatening messages from his/her account.
  - Spreading rumors about others through e-mail, instant messaging, text messages, or other network tools.
  - Using a website or social-networking account that targets another student or other person(s).
  - Sharing fake or embarrassing photos or videos of someone with others via a cellular device or the Internet.

Inappropriate Use for Staff

In addition to "Inappropriate Use for All Users," staff should not:

- Share their district password. The district password should not be shared with anyone, including other employees or the district technology department staff.
- Reuse their district password with other websites or services. Staff are encouraged to use a secure digital password manager. Efforts by district technology department staff to reduce the number of unique passwords needed by a user via password synchronization or other technologies is allowed and encouraged.

Inappropriate Use for Students

In addition to "Inappropriate Use for All Users," students should not:

- Reveal personal information such as their home address or phone number to other Internet users.
- Use their real name or any other information which might allow a person to locate the student without first obtaining the permission of a supervising teacher.
- Arrange a face-to-face meeting with someone "met" on the network or Internet.
- Buy or sell anything over the Internet.

Student Use and Filtering

Student access to the network and Internet is needed for achieving certain district teaching and learning outcomes. All student users and their parents or guardians are advised that access to the network and Internet may include the potential for access to materials inappropriate for school-aged students. District staff will take appropriate measures to monitor the online activities of students and to supervise student use of network and Internet access, but they must have student cooperation.

The district utilizes an Internet filtering system to prevent users from accessing websites with visual depictions that are obscene; pornographic; or, with respect to student use, harmful to minors. The district also prevents students from accessing other material that is inappropriate for school-aged students (as determined by district staff and school principals). Filtering systems have limitations and cannot be expected to be 100% effective. Filtering works with web browsing (not email or messaging) on equipment connected to the district networks. Devices connected to outside networks (such as student mobile phones with cellular Internet) cannot be filtered. Students will receive education about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Email Accounts and Archiving

The district will provide for qualifying students, qualifying staff, and school board members to access the district's email system. Messages on the system will be retained in an archived state for a minimum of three years for staff or school board members and one school year for students. A canceled account may not retain its email.

Student Email

All students are provided with district network and Google accounts. Student email is disabled on summer break excluding: (1) exceptions for special education students as determined by the district special education director, and (2) if needed for summer school students while summer school is in session.

Student email may be disabled during academic breaks.

Student email may be monitored by a third-party to alert the district to policy or safety concerns, but issues may only be addressed by district employees on days that school is in session from the hours of 8am to 4:30pm. The district encourages and supports parents/guardians to monitor their child's email account and their communications, but not to send email from their child's account.

Failure to Follow Policy

Users who violate this policy may lose access to the network or Internet in addition to other disciplinary actions in accordance with the district's discipline policies. In addition, violators and their parents/guardians may be subject to civil and criminal penalties as specified by Oklahoma and federal law.

Warranties/Indemnification

The school district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its networks and the Internet provided under this policy. The district and all staff shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user (or his/her parents or guardians) arising out of the use of its networks or the Internet under this policy. Users agree to indemnify and hold the school, the school district, the network or Internet provider, and all staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to the network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or the parent/guardians of a minor student agree to cooperate with the district in the event of an investigation of a user's network or Internet use, whether that use is on a school device or on a device outside the school district's network. Any expense incurred to access the district's network, servers, services, or software from a remote location, such as a home, is the responsibility of the user.

Privacy

The district reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the network and Internet and any and all information transmitted or received in connection with such usage. All such data shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials. Information may be used with third-party services to create accounts or reports for educational purposes, but only when approved by the superintendent or designee(s). Any data shared with third-parties will be the minimum required.

Records Retention: The District will retain its Internet Safety policy documentation for five years after the E-rate funding year in which the policy was relied upon to obtain E-rate funding.

REFERENCE: **21 O.S. §1040.75, §1040.76**
Children's Internet Protection Act of 2000 (HR 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [l])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)

THIS POLICY REQUIRED BY LAW.

~~**General:** Through the Internet, students and employees have access to e-mail, news, databases library resources, and a wide variety of other information sources. The District provides a wide variety of opportunities for students and employees to use the computers to access the Internet. Through the Internet, it is possible to access material that may contain illegal, defamatory, inaccurate, pornographic, and/or offensive content. Due to the nature of the Internet, the District cannot guarantee that students and employees will not access such material. However, the District is committed to enforcing a policy of Internet safety, teaching appropriate online behavior, and monitoring the Internet activities of its students and employees.~~
~~The District makes no warranties of any kind, either express or implied, regarding the Internet access being provided. The district shall not be responsible for any damages users suffer, including but not limited to loss of data resulting from delays or interruptions in service. Nor shall the District be liable for the accuracy, nature, or quality of information stored on District's computer equipment or of information gathered through~~

Internet access provided by the District. However, the Administration shall develop, implement, and maintain regulations and forms to restrict the use of the District's computers and Internet access to legitimate and acceptable purposes and to regulate students' and employees' privilege of access and use.

Acceptable Uses: The District's computers, equipment, and software are intended for administration, education, and academic research purposes only and shall be used only as according to administrative regulations. Acceptable uses of the District's computers and the Internet are activities which support learning and teaching or which promote the District's mission and goals.

Prohibited Uses: According to Administrative Regulations, the District's computers and the Internet access provided by the District shall not be used:
1. To violate an individual's right to privacy;
2. To access materials, information, or files of another person or organization without permission;
3. To violate the copyright laws;
4. To spread computer viruses or malware:
5. To deliberately attempt to vandalize, damage, disable, or disrupt the District's electronic property or the electronic property of any other individual or organization;
6. To locate, willingly receive, transmit, store, or print files or messages which are profane, obscene, or sexually explicit, or which use language that is offensive or degrading to others;
7. To distribute religions materials;
8. To campaign for or against any political candidate or ballot proposition.
9. For any commercial purpose resulting in personal gain or other commercial purposes not authorized by the Administration, Board or Board policies and regulations.
10. To engage in any illegal activity.
11. To engage in cyberbullying at school or in the workplace.

Consequences for Misuse: The use of the District's computers and/or the Internet access provided by the District is a privilege, not a right. Any student or employee who inappropriately uses District computers or devices, personally-owned devices, or the Internet through any other means may have the privilege of using electronic devices and access to the Internet or network denied, revoked, or suspended andmay be subject to other disciplinary sanctions.

No Expectation of Privacy: No student or employee shall have any expectation of privacy in any electronic mail being sent or received by the District's computers or the District-provided Internet access. The District's system operators may access any electronic mail and may remove any inappropriate material from any electronic mail sent or received using the District's computers or the District-provided Internet access. All Internet usage will be monitored and recorded to ensure compliance with the Children's Internet Protection Act ("CIPA"), as codified at 47 U.S.C. § 254.

Use of Software: Students are prohibited from installing, copying, or downloading any copyrighted or illegal obtained material or software on District's computer hardware. Employees are prohibited from installing, copying, or downloading any copyrighted or illegally obtained material or software on District's computer hardware without the express written consent of the copyright or license holder and the approval of the appropriate administrator or system operator.

Remote Internet-based Courses: The District may allow for students to complete required course work through remote Internet based courses in accordance with the rules, regulations, and/or guidelines adopted by the State Board of Education.

Internet-based Instruction: The District may allow for students to complete required coursework through Internet-based courses in accordance with the rules, regulations, and/or guidelines adopted by the State

~~Board of Education.~~

~~**Education:** The District will educate all students, who are granted access to the Internet, regarding appropriate online behavior including: safety and security when using electronic mail, interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness and response, and other forms of direct electronic communications, and the disclosure, use of dissemination of personally identifiable information.~~

~~**Web Filtering:** The District shall provide filtered access to the Internet per standards pursuant to CIPA.~~
~~Technology protection measures shall be in place that safeguard Internet access by users to visual depictions that are obscene, related to child pornography, or other content that may be deemed harmful to minors. The Board delegates to the Administration the authority to determine matter that is inappropriate for minors.~~
~~The District will enforce the operation of the technology protection measures on its computers with Internet access. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure during an audit, to enable access for bona fide research, or other lawful purposes.~~

~~**Records Retention:** The District will retain its Internet Safety policy documentation for five years after the E-rate funding year in which the policy was relied upon to obtain E-rate funding.~~