FAYETTEVILLE (AR) PUBLIC SCHOOLS
COMPUTER/NETWORK USE POLICY

The Fayetteville Board of Education recognizes the need to effectively use digital technology to further enhance the educational goals of the school district. Security of the various information networks and computer systems must be in place in order to ensure availability and reliability of the computer and network resources. All computing resources (to include desktops, laptops, and handhelds of all varieties) should be used in a responsible, effective, ethical, and lawful manner. Users are expected to learn and follow normal standards of polite conduct and responsible behavior in their use of computer resources.

The District shall provide Education to minors about appropriate online behavior, including: interacting with others on social networking sites and in chat rooms, and cyber bullying awareness and response. The Board further expects all faculty, students, and staff to use the district's computers and networks for the intended purposes of education, research, and administration. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communication.

All users of district equipment must sign the district computer and network use agreement stating they understand this policy and the guidelines contained in the administrative rules and procedures regarding computer use. Network accounts will not be assigned to a user until the use agreement is signed. If there is any doubt about whether a contemplated activity is in accordance with the purpose for which the account was provided, students should consult with parents and teachers and employees should check with immediate supervisors.

Violations of some guidelines set forth in the rules and procedures may constitute a criminal offense. Systems staff and district administrators will cooperate fully with law enforcement agencies in investigating any violations.

The district cannot be held liable for any losses, including lost revenues, or for any claims or demands against system users by another party. The district cannot be held responsible for any damages due to the loss of output, loss of data, time delay, system performance, software performance, incorrect advice, or any other damages arising from the use of the district's computer facilities or equipment. Faculty, staff, students and/or their parent or guardian will be held liable for any of the above that he/she causes.

It is the responsibility of each user on the network to recognize his/her accountability in having access to vast services, sites, systems and people, and to act according to acceptable behavior standards when using the network. It is necessary that users observe the Acceptable Use Policy of other networks as well as this policy.

System users must not obtain, attempt to obtain, or disseminate any electronic communication or information not intended for them, or directly related to the responsibilities they are assigned.

Use of the district's computers and access to the network is a privilege that will be revoked for violation of any of the administrative rules and procedures listed below. Users are subject to appropriate disciplinary measures, up to and including non-renewal, termination and expulsion should these guidelines be violated.

All computers remain under the control, custody, and supervision of the district through management and oversight by the district Technology Department. Under normal circumstances, the district will not monitor or inspect email or web transaction logs as standard operating procedure. However, if there are legal or disciplinary issues that require the district to monitor, inspect, copy, or review files maintained on district computers or networks, the district reserves the right to do so. All such information shall be and remain the property of the district and no user shall have any expectation of privacy regarding such materials. Email is subject to Freedom of Information (FOI) requests.

RULES AND REGULATIONS FOR USE OF COMPUTER/NETWORK RESOURCES

I. INTERNET SAFETY

A) **General Warning: Individual Responsibility of Parents and Users.**

All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for children and minors. Even though filters are in place (see E, below, "Active Restriction Measures"), they are an imperfect means of blocking access to inappropriate material. If a user unintentionally visits an offensive or harmful site, he or she should bring this to the attention of the supervising teacher who should then report it to the district system administrator. Every user must take responsibility for his or her use of the computer network and Internet and stay away from inappropriate sites. Parents of minors are the best guide for materials to shun. If a user finds that other users are visiting offensive or harmful sites, he or she should bring this to the attention of their teacher or supervisor.

B) **Personal Safety for students.**

In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information that might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parent's permission (if you are under 18).

C) **Confidentiality of Student Information and Personal Information.**

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. See the exception regarding "directory data" here:
http://www.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html
Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers.

D**) "Hacking", "Spamming", and Other Illegal Activities**

It is a violation of Policy 4202 to use the districts computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to trespass, copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

E) **Active Restriction Measures**

The School, either by itself or in combination with the State of Arkansas Department of Information Systems (DIS) providing Internet access, will utilize filtering software or other technologies to prevent students from accessing materials/sites that (1) are obscene, (2) contain child pornography, or (3) could be harmful to minors. The School will also monitor the online activities of students, through direct observation, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors. Monitoring through technical means will only be used in special circumstances if it is necessary to track documented violations. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

F) **Failure to Follow Policy**

Use of the computer network and Internet for education, research, administration, and incidental personal use is a privilege, not a right. A user who violates Policy 4202, shall, at a minimum, have his or her access to the computer network and Internet terminated, which the district may refuse to reinstate for the remainder of the student's enrollment or staff member's employment. A user violates the Policy by his or her own action and should understand that it is a personal responsibility to report any violations by others that come to their attention. Further, a user violates the Policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The district may also take other disciplinary action in such circumstances.

II. BEHAVIOR STANDARDS

A) Users are expected to behave in a moral, legal, and ethical fashion that supports district education goals.

B) Abusive conduct when using the computer or network is prohibited.

Abusive conduct can be, but is not limited to:

1) Placing of unlawful information on the system
2) Using abusive, obscene, threatening or objectionable language.
3) Sending messages that are likely to result in the loss of recipient's work or systems.
4) Sending of "chain letters," or "broadcast" messages to lists or individuals.
5) Use of the system to intimidate or create an atmosphere of harassment.

C) Interference with or disruption of the network users, services, or equipment is prohibited.

Disruptions could include, but are not limited to:

1) Distribution of unsolicited advertising.
2) Propagation of computer worms or viruses.
3) Unauthorized entry to any other machine accessible via the network.
4) Attempting to degrade or degrading system performance.

D) Transmission of any material in violation of any U.S. or state laws or regulations is prohibited and may constitute a criminal offense.

E) Accessing another individual's electronic mail is prohibited except when an investigation requires the monitoring of systems by authorized technology staff.

F) Attempts to gain unauthorized access to systems is prohibited.

G) The use of another individual's access codes/passwords is prohibited.

H) Copying of another individual's work or copyrighted material is prohibited.

I) Use of the computer system or network for commercial or promotional purposes is prohibited, except as provided by the district Message Board.

III. THE COMPUTER NETWORK

The district network and any access to the larger information networks exists for the primary purpose of transmitting and sharing information between academic and research organizations.

A) All computers from which electronic information resources can be accessed by students will be in supervised areas. District staff shall monitor student computer use, providing assistance or taking corrective action when necessary.

B) Designated district staff shall assist in providing:

® Training for students and other staff in the appropriate and safe use of remote electronic information resources.
® Instructions to students and staff on the responsible use of on-line resources.
® Direction to on-line resources that relate to curriculum, teaching and learning, and related communications priority activities and applications.

C) Network use must be consistent with the goals and standards of the district, school, and specific curriculum.

D) Networked computers may be used as a laboratory for research and experimentation in computer communications and curriculum development where such use does not interfere with normal operations.

E) Faculty, students, staff and associates are individually responsible for the proper use of their accounts, including proper password protection and appropriate use of network resources. Users are expected to protect their accounts from being used by anyone else.

F) An account assigned to an individual shall be used by that individual only. Teachers will not provide network access to a student through a teacher account.

G) To ensure security and prevent unauthorized access to account privileges, users must log off the network any time they cannot monitor the use of their machine.

IV. USE OF COMPUTER HARDWARE

A) Only individuals authorized by the district Technology Department will install, service, and/or maintain district-owned computer hardware.

B) No hardware, including cables or peripherals, may be moved without authorization from district Technology Staff.

C) It is the responsibility of the faculty member to whom the computer is assigned to shut down their computer system at the end of each day. It is the responsibility of the faculty, students, staff, and associates to make reasonable efforts to keep the computer clean and away from smoke, dust, magnets, food, liquid, and any other foreign material known to be harmful to the hardware or functionality of the system.

D) It is the responsibility of the faculty member to whom the computer is assigned to report malfunctions of the hardware to the site technology specialist using appropriate reporting method.

E) The district is not responsible for the loss of any data on the local drives. Data on the local drives is not secure and your local drives may be reformatted at any

time. In order to secure data, all data must be saved to a location on the network .e. home directory or shared directories.

V. USE OF COMPUTER SOFTWARE

A) Only software that is legally owned or authorized by the district may be installed on district computer hardware.

B) The unlawful copying of any copyrighted software and/or its use on district hardware is prohibited.

C) Modification or erasure of software without authorization is prohibited.

D) The introduction of any viral agent is prohibited. All media should be checked for a virus each time it is put into the computer system.

E) The technology staff has the right to remove any software from district owned equipment where the user cannot provide original copies of the software and/or appropriate license for the software.

F) The technology staff has the right to remove any software from district owned equipment that degrades the performance of the equipment, the operating system or the network.

G) All software purchased with district funds must be maintained under district accounts and made available to district technology staff for the purpose of installation and recovery if necessary.

VI. PROPER RESPECT FOR COPYRIGHT

In an effort to encourage the proper respect for copyright on the Internet, the following guide for staff and student users is provided:

• If the user did not create a non-public domain written work, piece of art, photograph or music, or obtain rights to it, THE USER DOES NOT OWN IT.

• If the user does not own the non-public domain material, the user may not copy it or distribute it to others.

• The author or owner of a document or other type of information must explicitly relinquish rights in order to place a work in the “Public Domain” and thereby make copying/distribution with specific authorization possible.

• *Fair use* allows the user to copy small portions of a work the user does not own without permission, but only for criticism, education, news reporting, and the like.

• When in doubt, the user should ask the creator or owner of material for permission to use the work.

- Content that is licensed for use by the copyright holder may be used only as long as the license for use remains in effect. Once any licenses to use content expire or are revoked, that content may no longer be legally used for any purposes that are not considered *Fair Use* or otherwise exempted from copyright restrictions.

VII. SOCIAL MEDIA GUIDELINES

Employees and students should be mindful of the information they post. Online behavior should reflect the same standards as those used for face-to-face communications. Deleted information may be stored and retrieved indefinitely. Information marked "private" rarely is, and may be forwarded easily, even by someone you trust. Share ideas in a respectful manner.

Guidelines for All Users

- Respect student and employee privacy rights and laws. Do not comment on students or confidential student matters on social networks
- View online content, including social media, as an extension of your physical classroom or building. If it is not appropriate in the classroom or out in the open at school, it is not appropriate online either.
- Search your name online and monitor what others are saying and posting about you. Even your friends and family can post and tag (i.e., identify you by name) photos you would never consider making public. If that happens, either ask the person to remove the offending photo or make it clear that you do not support its publication. Be sure to review your privacy settings regularly.

Guidelines for Employees

- Ensure that content reflects and is consistent with the work you do for your district. Once you identify yourself as a school or district employee, you are automatically connected with colleagues nationwide.
- Do not use e-mail, text messaging, instant messaging, or social networking sites to discuss non-school-related issues with students. Homework, class activities, athletics, extracurricular activities, parent nights, choral concerts, and other school activities represent appropriate topics of discussion. Keep relationships with students professional at all times.
- Do not violate your co-workers' privacy. Professionals have tough conversations face-to-face and in the appropriate settings.
- Identify yourself as a school employee, and do not post comments anonymously

or try to hide your role. Fact-check information for accuracy before posting or sending it to another person.

Approved: 6/27/02
Revised: 5/23/02
Revised: 6/24/04
Revised: 6/23/05
Revised: 3/13/09
Revised: 5/26/11
Revised: 3/28/13 Effective Date: 7/1/13