2. State that the views expressed are not necessarily those of the School Board or the employees of the District.

Student Media may be distributed at the following times and places:

1. Before and after school;
2. At recess;
3. During school hours, but only passively at designated tables;
4. In the hallways during non-instructional time, but only at middle and secondary schools:
5. In the cafeterias during non-instructional time and designated lunch periods, but only at middle and secondary schools; and
6. As further authorized by a building principal in a manner that is content and viewpoint neutral and that does not cause a substantial disruption of the orderly education environment.

Student Distribution of Non-school Literature, Publications, and Materials

A student or group of students who distribute ten or fewer copies of the same non-school literature, publications, or materials (hereinafter "non-school materials"), shall do so in a time, place, and manner that does not cause a substantial disruption of the orderly education environment. A student or group of students wishing to distribute more than ten copies of non-school materials shall have school authorities review their non-school materials at least three school days in advance of their desired time of dissemination. School authorities shall review the non-school materials, prior to their distribution and will bar from distribution those non- school materials that are obscene, libelous, pervasively indecent, or advertise unlawful products or services. Material may also be barred from distribution if there is evidence that reasonably supports a forecast that a substantial disruption of the orderly operation of the school or educational environment will likely result from the distribution. Concerns related to any denial of distribution by the principal shall be heard by the Superintendent, whose decision shall be final. The time, place, and manner for distributing non-school materials is governed by the time, place, and manner provisions for distributing Student Media.

Legal References: A.C.A. §§ 6-18-1202, 1203, 1204
Tinker v. Des Moines ISD, 393 U.S. 503 (1969)
Bethel School District No. 403 v. Fraser, 478 U.S. 675 (1986)
Hazelwood School District v. Kuhlmeier, 484 U.S. 260 (1988)

Additional Reference: ASBA Model Policies
Date Adopted: 5-20-2019
Date Revised:

XII. FORT SMITH PUBLIC SCHOOLS NETWORK/INTERNET ACCEPTABLE USE GUIDELINES

A. Acceptable Use

The Fort Smith Public Schools' digital devices, networks and Internet access are provided to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying rules also apply to digital devices issued directly to students, whether in use at school or off school premises.

Students are allowed to use privately-owned devices at school with prior authorization by school officials, provided that they comply with this policy and the accompanying rules.

B. Unacceptable Use (ACA 6-21-107)

The District has established and will maintain an Internet filtering system to prevent computer users from accessing harmful material. The use of the network is a privilege, not a right, which may be revoked at any time for inappropriate conduct as determined by the Fort Smith Public School District.

Such conduct would include, but not be limited to, the placing or viewing of unauthorized or unlawful information (data or graphics) on a system, messages/data, the sending of messages/data that are likely to result in the loss of a recipient's work or systems, and the sending of "chain letters," or "broadcast" messages to lists or individuals. District computing resources cannot be used to intimidate or create an atmosphere of harassment based upon gender, race, religion, ethnic origin, creed, or sexual orientation. The unauthorized disclosure, use, and/or dissemination of personal identification information regarding students or staff is strictly prohibited. Any unauthorized access to District, staff, or student information by any individual is prohibited.

It is essential for each user on the network to recognize his/her responsibility in having access to vast services, sites, systems, and people. The user is ultimately responsible for his/her actions in accessing network services. Users must also observe the acceptable use of policy of other networks. What is acceptable use on the District network may not be acceptable on outside networks.

An account assigned to an individual, including Student Use Accounts, may not be used by others. Faculty, students, staff, and associates are individually responsible for the proper use of their accounts, including proper password protection and appropriate use of Internet resources. It is not acceptable to use the network to interfere with or disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation or computer worms or viruses, and using the network to make unauthorized entry to any other machine/service accessible via the network. No one should deliberately attempt to degrade the performance of a computer system (including network resources) or to deprive authorized users of resources or access. Use of the network for recreational games is not acceptable.

C. Behavior in Use

All faculty, students, staff, and associates are responsible for use of district computing resources in an effective, efficient, ethical, and lawful manner even in the absence of reminders or enforcement. Users are expected to follow normal standards of polite conduct in their use of the computing resources. Responsible behavior includes consideration for other users, as well as efficient use of the computing time and materials. Annually every user will be required to successfully complete training as defined by the School District in order to be eligible to access network services.

The District cannot be held liable for any losses, including lost revenues, or for any claims or demands against the user by another party. Users are personally monetarily responsible for their unauthorized access to any "pay" service. 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 from a consultant, or any other damages arising from the use of the District's computer facilities.

Faculty cannot be held liable for the student's use of the network. Students may access the network for individual work, in the context of another class, at a location other than on campus. The faculty is responsible for instructing and supervising students on acceptable use of the network, network etiquette, electronic mail, chat rooms, and other forms of electronic communication. **Students have no expectation of privacy in their use of school digital devices.**

D. Plagiarism

Copying a student's computer assignment takes little effort; as does detecting and proving such plagiarism. The standard academic penalties for this are severe. Systems staff will cooperate with instructors in verifying plagiarism. Guilty users will lose computing privileges. Students may be subject to receiving a failure for the assignment and possible failure for the course. This includes students who have completed a course and shared their old work with those in a subsequent semester.

E. Use of Copyrighted/Licensed Materials

Unauthorized copying, transmittal of, or use of licensed or copyrighted media (example: software) is considered theft and a violation of copyright laws. Placement of media (example: software onto an on-site user's computer hard disk) onto School District information systems equipment should not be done without prior authorization. Final responsibility of management of a given piece of equipment and the media placed on it is held by the assigned user or on-site lab supervisor.

F. Violations Statement

Violations of the guidelines set forth in this policy shall constitute a violation of school rules and will result in punishment of the student with a minimum penalty of a reprimand to a maximum penalty of expulsion.

Violations of some of the guidelines set forth in this policy may constitute a criminal offense. Transmission or use of any material in violation of any international, U.S., or state laws or regulations is prohibited. Systems staff and district administrators will cooperate fully with law enforcement agencies in correcting any violations.

G. Online Safety Pledge

The student's signature on the District's Student Handbook signature page indicates she/he will uphold all aspects of the following pledge.

I want to use the computer and the Internet. I understand that there are certain rules about what I should do online. I agree to follow these rules:

1. I will not give my name, address, telephone number, school, or my teachers'/parents' names, addresses, or telephone number to anyone I meet on the Internet.
2. I will not give out my email password to anyone (even my best friends) other than my teachers/parents.
3. I will not send a picture of myself or others over the Internet.
4. I will not fill out any form or request online that asks me for any information about my school, my family, or me.
5. I will tell my teachers/parents if I see any bad language or pictures on the Internet, or if anyone makes me feel nervous or uncomfortable online.
6. I will never agree to get together with someone I "meet" online.
7. I will not use any articles, stories, or other works I find online and pretend it is my own.
8. I will not use bad language online.

9. I will practice safe computing, and check for viruses whenever I borrow a disk from someone, download something from the Internet, or receive an attachment.

10. I will be a good online citizen and not participate in any activity that hurts others or is against the law or my school's policy.

11. I have no expectation of privacy in my use of school digital devices.

H. Additional Rules for Digital Devices Issued to Students for Classroom Use

1. Digital devices are loaned to students as an educational tool and are only authorizedfor use in completing school assignments.

2. Students are responsible for the proper care of digital devices at all times, whether on or off school property, including costs associated with repairing or replacing the digital device.

3. If a digital device is lost or stolen, this must be reported to the schools administrators immediately. If a digital device is stolen, a report should be made to the local police and to district administrators immediately.

4. The Board's policy and rules concerning computer and internet use apply to use of digital devices at any time or place, on or off school property.

5. Students are responsible for obeying any additional rules concerning care of digital devices issued by school staff.
6. Violation of policies or rules governing the use of digital devices, or any careless use of a digital device may result in a student's digital device being confiscated and/or a student only being allowed to use the digital device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.

7. Parents will be informed of their child's login password. Parents are responsible for supervising their child's use of the digital device and Internet access when in use at home.

8. Digital devices must be returned in acceptable working order at the end of each use, or whenever requested by school staff.

9. Students who are issued a Fort Smith Public Schools email address should have no expectation of privacy in its use. Parents may request to be given access to student email accounts by completing a Parental Request for Access to Student Email Account from the Director of Technology at Rogers Center (784-8130).

I. Additional Rules for Bring Your Own Device (BYOD)

1. Students are expected to use these devices only for educational purposes during school hours. Teachers have the right to require a student not to use the device if they believe that it is being used for anything other than educational purposes.

2. Students must login with their assigned unique username and password before accessing the wireless network.

3. Students have no expectation of privacy in their use of a privately-owned device while at school. The school unit reserves the right to search a student's privately-owned devices if there is reasonable suspicion that the student has violated Board policies, administrative procedures or school rules, or engaged in other misconduct while using the device.

4. Whether or not student-owned devices are permitted to be used in the classroom during instructional time will be determined by the individual teacher.

5. If a student is caught violating the acceptable use policy, his or her access may be revoked temporarily or as decided by the building principal or administrator.

6. The Fort Smith School District will not be held financially or legally responsible for lost, stolen, or damaged devices.

7. Support will not be provided by the Technology Department or Technology Liaisons for student-owned devices if they are unable to connect. **Students have no expectation of privacy in their use of a privately-owned device while at school.**

8. The school unit may confiscate any privately-owned device used by a student in school without authorization as required by these rules. The contents of the device may be searched in accordance with applicable laws and policies.

J. Internet Safety and Web Filtering Policy

The Fort Smith Public School District has developed a set of policies and guidelines to address the Internet safety of both students and staff members. These guidelines follow security guidelines as recommended by the Department of Information Systems of the State of Arkansas and the Arkansas Public School Computer Network Division. They are also in compliance with the Child Internet Protection Act.

1. Web filtering servers will be employed, updated and maintained to prevent access by minors to inappropriate subject matter on the Internet and the Web.

2. The use of electronic mail, chat rooms, or any other form of direct electronic communications by students will be prohibited unless monitored by a staff member to protect the students' safety and security.

3. A network firewall will be employed, updated, and maintained to prevent unlawful or unauthorized access, including "hacking", from the outside or from within the computer network.

4. Information security access rules and secure password policies will be employed to prevent the unauthorized disclosure, use, or dissemination of personal identification information regarding students and staff members.

5. Student access to materials harmful to them will be restricted through the implementation of web filtering servers, a network firewall, and anti-malware software.