EMPLOYEE ACCEPTABLE USE POLICY 4.406-A

PURPOSE AND PROPER USE

Employee access to computers and the Internet is provided to support the school system's educational mission, curriculum and instructional goals. The system's computer technology is not to be used for private financial gain, commercial advertising or solicitation. Employees are expected to maintain all equipment issued to them in good working order and conduct themselves professionally, safely and securely while online.

STUDENT AND EMPLOYEE SAFETY

All employees must take steps to safeguard sensitive data in e-mails and chats, files they share, websites they visit, and social media accounts they frequent. This data includes, but is not limited to, students' full names, contact information, photographs, personally identifying numbers such as social security numbers, and health conditions. Unauthorized release of this information is a violation not only of board policy but of state and federal law.

To help safeguard sensitive information, employees must use strong passwords. Passwords will be at least twelve characters long and should consist of something memorable that will not need to be written down. Sharing passwords or accessing another user's account is prohibited. Employees with access to sensitive data must utilize two factor authentication on all public facing accounts where available. Employees must not store or transport sensitive data except on encrypted media.

Student information such as a student's name or likeness will not be released without written parental consent. This consent will be kept on file at the school the student attends.

EMAIL AND CHAT

All employees of the school system must use the official email and chat systems provided for this purpose for all district-related communications. All e-mail, chat and other data stored or transmitted through the school system's network will be monitored and employees have no privacy with regard to such data. When using e-mail or chat keep in mind that any school correspondence may be a public record under the public records law and be subject to public inspection.

SOCIAL NETWORKING

Employees who have a personal or institutional presence on social networking websites are prohibited from posting data, documents, photographs or inappropriate information that is likely to create a material and substantial disruption of classroom activity. Employees are prohibited from accessing personal social networking sites on school computers or on personal devices during school hours except for legitimate instructional purposes. The Board discourages district staff from socializing with students on social networking websites. The same relationships, exchanges, interactions or behaviors that would be unacceptable in a non-technological medium are equally unacceptable in a technological one.

The same system policies that govern employee conduct and communication apply to the use of technology. Web publishing, chat groups, blogging, podcasting, wikis and similar technologies used by an employee must be treated like a school publication representing the system. All language and content restrictions must be followed.

FILTERING AND MONITORING

Although filtering software is in place, computer security cannot be made perfect--some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive. If offensive material is encountered it is the responsibility of the employee to leave the offensive site immediately and report it to the Technology Department. In a classroom setting the supervising teacher will monitor all computer activity of students under their guidance to ensure non-violation of the Student Acceptable Use Policy. The school system reserves the right to monitor the technology use of all employees to enforce this Acceptable Use Policy. There should be no expectation of privacy while using district computers or the district's network.

ABUSE AND ILLEGAL ACTIVITY

The district's technology will not be used to harass, defame, intimidate, threaten, discriminate against or otherwise harm other individuals or groups. This includes accessing, submitting, posting, forwarding, scanning or displaying any offensive or obscene material by any method. In addition to violating Board policy and this Acceptable Use Policy such acts may be prosecuted under Federal and State laws.

Any tampering, hacking of, disruption or harm to the system's computers, networks and other technology will be considered a violation of Board policy and be punishable through computer access revocation, disciplinary action and/or criminal prosecution

depending on the infraction. All costs incurred by the school or district because of loss or damage to technology equipment due to a violation of this policy will be the responsibility of the employee.

Violation of copyright law is expressly prohibited. When Internet sources are used by an employee or student , the author, website and publisher must be identified.

Any malfunctioning technology, suspected breach of security or illegal activity must be reported to the Technology Department using the ticketing system the department has provided.

PERSONAL DEVICES, MEDIA AND SOFTWARE

Aside from the customization of an employee's computer desktop or similar digital working space, no personal media (music, video or pictures) not for educational use are allowed on any district computer. Only software intended for educational use may be installed on any district device and this software must be approved by the Technology Department. All media and software must be properly licensed by the copyright holder or by legal Fair Use.

Personal portable devices such as smartphones, tablets, Chromebooks or Macintosh laptops may be connected to the district's wireless network. All other wireless devices must be approved by the Technology Department. No device may be attached to the district's wired network without authorization from the Technology Department. Any unauthorized device found connected to the district network may be confiscated with disciplinary action to follow. Donated devices must have prior approval from the school administrative office and the Technology Department before use in the classroom or office.

INVENTORY

Employees are responsible for all technology assigned to their classroom or office and will submit an inventory of that technology to the Technology Department at the completion of each school year.

DISCLAIMER

The Fayetteville City School System will not be responsible for any loss of data, interruption of service, or the accuracy or quality of the information obtained through or stored on the Internet. The Fayetteville City School System will not be responsible for financial obligations arising through the unauthorized use of the network. Fayetteville City School System reserves the right to modify these guidelines as deemed necessary to provide a safe and secure environment for employees and students. Upon termination of employment with the school system any devices issued to that employee must be turned in to the Technology Supervisor and all access to information systems will be terminated.

By signing this contract, I hereby acknowledge that this is a legally binding document and I have a thorough understanding of the Employee Acceptable Use Policy of the Fayetteville City School System and agree to abide by all of the terms and conditions listed herein. I further understand that a violation of the Employee Acceptable Use Policy may result in disciplinary action, including, but not limited to, the loss of privilege to use the system's information technology resources and/or legal prosecution. I also further understand that this document will remain in effect during my entire employment with the Fayetteville City School System.

______________________________________ ______________________________________

Employee Signature **Date**

____

Employee's Printed Name

UPDATED 5/31/2019