School District Acceptable Use Policy

The Little Rock School District has policies in place that address all CIPA and FERPA laws. Guidelines regulating the use of the District Network (Acceptable Use Policy) also include policies and consequences for violation of policies posted on the LRSD website and printed in the student handbook. Students, parents, all employees and users must sign this agreement if they are to use the district network. A handbook is issued to every student at pre-school registration and upon entering the school district. New employees are issued the agreement upon employment.

This policy governs the acceptable use of district technology by all users. User access is a privilege with no entitlement guaranteed and access may be revoked at any time at the discretion of the superintendent or other administrative authorities. As an administrative authority for the Little Rock School District, the Little Rock School District Board of Directors is authorized to make CIPA certifications policy. This policy may be revised at any time by a two-thirds vote of the LRSD School Board of Directors or as state and federal law dictates.

A security audit of our network is conducted every three-four years. Filters and firewalls are tested against the most severe violations breaches to determine the strength of the network.

I. Purpose

The Internet and its vast access to information provide an enormous resource for education and assistance in our goal to increase student achievement and professional development. The computer, mobile devices and other computer related technologies and software are valuable tools in the efforts to provide a quality educational process. This, combined with the need of creating and maintaining a safe educational environment require an adequate acceptable use policy for the Little Rock School District.

Little Rock School District Responsibilities

The Little Rock School District will take the following steps to assure proper use of the computer network:

- Teachers and/or support staff will supervise Internet sessions while in the classroom or computer lab.
- Filtering and network management software will be used to limit the risk of in appropriate material being accessed by students and other users. These programs monitor ‘http’ traffic and block inappropriate content based on an expanding database of sites and information related to trends in best practices, known information and constant system monitoring.
- Teachers will be provided with training and resources to understand the current trends and policies of Internet usage and safety practices.
- Staff will be required to instruct students on the proper use of Internet resources enabling them to make appropriate choices for appropriate content and its use.
- Current virus protection and anti-malware software will be used as an added layer of protection for users against malicious software that may otherwise expose students and other users to inappropriate or harmful material.

Definitions

Internet: A network of computer networks. Networks in the Internet are connected so they can communicate with each other regardless of their manufacturer.

Mobile Devices: Portable hand held computing device that mimics desktop computers in their function. These devices include Wi-Fi capability and may or may not have a touch screen, keyboard or cellular data connections. Users may access Internet content, email, stream video and have access to take and or post electronic photos/videos. Devices include, but are not limited to tablet devices, smart phones and e-readers.

Asynchronous Communication: A type of communication protocol that allows an amount of time to pass between communications.These communications include, but are not limited to emails, discussion forums,weblogs (blogs) and social networking sites (MySpace, Facebook, etc).

Synchronous Communication: A type of communication protocol that allows users to communicate instantly in real time. These communications include, but are not limited to chat rooms, instant messages, voice over IP, virtual field trips and certain 3D environments such as *"Second Life".*

Users

a. Users are defined as authorized personnel as defined by the Little Rock School District to operate

computers,computer-related devices and other technology related equipment within the boundary of the District.

b. Users are described but not limited to: administrators, teachers, students,¡.substitutes,long-term substitutes, parents, support staff and District, authorized guests who are identified as vendors and presenters.

c. The amount of access to the District equipment and network for each of.these uses will be determined by function and need by the appropriate personnel.

d. Any user 17 years of age and under, is considered a minor as defined by federal law.

Social Networks: Websites that are "virtual communities" of people with common interest who are invited to share likes and dislikes on any particular subject, cause and/or theme or to have an online meeting place for extemporaneous discussion. Members create accounts that consist of biographical information including but not limited to birthdays, gender, photos, occupation and email addresses. Communication consists of both synchronous and asynchronous communication such as chat, voice over IP, blogs, email, discussion forums, mobile devices and video.

Mobile Apps (Mobile Applications): Programs specifically designed to run on mobile devices that at times mimic desktop computer programs. These applications may or may not need Internet access. These programs range from games to productivity applications.

Malware: Various types of computer programs that use various techniques to duplicate themselves and travel between computers which can cause serious damage to computers such as erasing important data or disrupting a system or network.These programs may collect personal information about the user for exploitation which may or may not be for financial gain.

Elementary School

An elementary school, in the LRSD, is a public entity under the governance of the LRSD Board of Directors that provide education according to state law to students in grades PK-5 .

Secondary School

A secondary school, in the LRSD, is a public entity under the governance of the LRSD Board of Directors that house grades 6-12 and provide education according to state law to students in grades 6-12.

Federal Guidelines

CIPA- Children's Internet Protection Act

In order to comply with comply with CIPA Guidelines, the Little Rock School District Board of Directors governs Internet access for students and staff as follow:

Under CIPA, schools and libraries subject to CIPA do not receive the discount offered by the "E-Rate"program (discounts that make access to the Internet affordable to schools and libraries) unless they certify that they have certain Internet safety measures in place.

These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography or (c)when computers with Internet access are used by minors, are harmful to minors;

Schools subject to CIPA are required to adopt a policy to monitor online activities of minors; and

- Schools and libraries subject to CIPA are required to adopt a policy addressing: (a) access by minors to inappropriate matter on the Internet and World Wide Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online;(d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.

The Little Rock School District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, cyber bullying and response through the following means:

- Instruction by, and not limited to, Library Media Specialists and technology instructors, using ADE Library Frameworks for proper online safety; Connect with Kids Web source for online safety; Common Sense resources, and Gaggle online safety mini course (see appendix D for example).
- All users will read and sign the AUP prior to logging in to any device on the district network. Parents of minors will also be required to sign the AUP acknowledging their awareness of student responsibility for network and equipment use as well as consequences of unacceptable use of the network and equipment. The AUP will be signed upon entering any LRSD school and remain in effect for the tenure of that site unless the AUP is revised. Students transferring to a different site or entering a new site after the beginning of the school year will be required to sign a new agreement.
- Filtering and network management software is in place to limit the risk of inappropriate material being accessed by students and other users.
- Student email accounts will be furnished through the district approved provider, Gaggle. These accounts are filtered and monitored through LRSD personnel and the provider. Suspect email messages are blocked and forwarded to the LRSD Account Manager for disciplinary action, when required.

FERPA- Family Educational Rights Privacy Act

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFRPart 99) is a Federal law that protects the privacy of student educational records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

•FERPA gives parents certain rights with respect to their children's educational records. These rights transfer to the student when he or she reaches the age of18 or attends a school beyond the high school level. Students to whom the right has transferred are "eligible students."

Copyright: Copyright is a form of protection provided by the laws of the United States (title 17, *U. S. Code)* to the authors of “original works of authorship,"including literary, dramatic, musical,artistic, and certain other intellectual works.

This protection is available to both published and unpublished works.

The Digital Millennium Copyright Act (DMCA) passed in 1998 to protect software copyright holders, as well as owners of other digital media, from illegal copying of their products. Among other things, the DMCA 1) prohibits circumventing commercial software's anti-copying or anti-piracy measures; 2) prohibits the "manufacture, sale, or distribution" of programs or devices used to circumvent software's anti-piracy measures, except when these items or programs are used to test anti-piracy measures or to conduct research on encryption; 3) allows nonprofit libraries, archives and educational institutions to make copies of software that is otherwise protected by anti-piracy measures; and 4) requires Internet service providers to remove software programs posted to users' websites, if the programs appear to be posted in violation of copyright. The fair use provisions of the Copyright Act are still available to individuals charged with copyright infringement under the DMCA.

Fair Use: One of the rights accorded to the owner of copyright is the right to reproduce or to authorize others to reproduce the work in copies or phono records. This right is subject to certain limitations found in sections 107 through 118 of the copyright law (title 17, U. S. Code). One of the more important limitations is the doctrine of "fair use.” The doctrine of fair use has developed through a substantial number of court decisions over the years and has been codified in section 107 of the copyright law. Section 107 contains a list of the various purposes for which the reproduction of a particular work may be considered fair use: for the purpose of researching and teaching.

Illegal Behavior: Defined as use that violates all applicable laws, municipal ordinances, state and federal law which includes, but are not limited to gaining unauthorized access to district computers, systems and networks or attempting to gain unauthorized access, copyright violations, distribution of pornography or obscene material,the creation and distribution of malicious code (malware) and theft either on district or personal devices while on district property. Other types of illegal violations include,but are not limited to:

Flaming: To send an e-mail message to others that is abusive and/or offensive. Typing in all capital letters is considered shouting and may be offensive.

Spamming: To send an annoying or unnecessary message to a largenumber of people. An example might be a chain letter asking a user to forward the message to x number of people.

Cyber bullying: The intentional act of posting, transmitting or displaying of embarrassing,defaming and/or untrue information about a particular person or persons for the purpose of causing intimidation, ridicule, threat, harassment and/or an act of violence towards a student or public school employee. This behavior substantially disrupts the educational process within the classroom, overall school climate and the orderly operation of the school and the educational environment. The information is communicated through all forms of electronic communication including but not limited to text messaging, weblogs, podcast and social networking sites such as but not limited to MySpace, Face Book, and YouTube.

II. Regulations

General

1. Mobile devices,computers, computer related devices, telephonic and other communication devices and networks are provided for conducting school business and are for the educational development of students and staff.They are not intended for private or personal use. Internet and other network communications are being monitored for effective use and resource management. Users and their immediate supervisors may be notified of suspected abuse of network resources.

2. Users of the network are responsible for following local, state, federal and international laws. This includes copyright laws.

3. Users are responsible for the use of their own account, including security and proper use. Users are not to allow others to use their username and password. Access to other user profiles is reserved for authorized network administrators. Users assigned usernames and passwords are responsible for safeguarding this information. This includes posting account/passwords and access codes in public view or giving unauthorized users such as but not limited to students, parents or vendors access to the district network resources. Users in violation will be held accountable for the consequences of intentional or negligent disclosure of this information.

4. Users may not store student or employee personal data on their personal computing,mobile or storage device.

5. Users are restricted from viewing, downloading or sharing pornographic, sexually explicit, obscene and/or inappropriate content using personal mobile devices in the presence of other users, on school district property and/or while performing school district business.

6. Users may not gain unauthorized access or attempt to gain unauthorized access to other users' accounts, computers or devices.

7. Users are responsible for respecting the policies of other networks, which they access and for adhering to those policies.

8. Users may not deliberately damage or attempt to damage or disrupt **(otherwise known as hacking)** a network, computer or computer related device, telephonic or other communication device, and/or removable media that they have been given authorized use.System components such as hardware, software or other property will not be installed, removed, destroyed, modified or abused. Examples of activities that are prohibited: altering security codes or passwords and introducing computer viruses and/or malware, removing memory chips, hard drives and other hardware components.

9. No LRSD network, phone, mobile device or computer system will be used to terrorize, intimidate, threaten or harass.

10. Users will not use the LRSD network or resources for financial or commercial gain or to advertise, promote or endorse products or personal services.

11. The District will not be responsible for financial obligations or legal infractions arising from unauthorized use of the system.

12. Network resources, information, Internet and intranet traffic, folders, drives and mobile devices District provided removable media and electronic mail have no expectation of privacy. Routine maintenance and monitoring of the system may lead to the discovery that a violation of a law or regulation has occurred. If there is reasonable suspicion that a law or regulation has been violated, an investigation will be conducted and items seized and searched.

13. Long-term substitutes may be granted network privileges at the request of the building principal. If granted, the long-term substitute must sign the Authorized Use Policy.

Hardware

14. Only authorized individuals will service or maintain District owned hardware.

15. All personal hardware such as media players of any kind and their content are subject to LRSD policies that refer to electronic communication devices.

Software

16. Only software that is authorized by the District may be installed on computer hardware.

17. Only authorized individuals will install or remove software on District equipment. The district holds the right to remove any software that violates district software policy, software that is deemed illegal or inappropriate, or degrades network performance.

18. Authorized user of student and employee data will take proper care to guard the privacy of such information. Any violation of privacy to such information should be reported to authorities immediately.

19 .Mobile Apps that are to be purchased for use in the classroom must be submitted for software approval before purchase.

Internet Access and Email

20.The primary purpose of providing Internet access to employees is for conducting official business. The purpose of providing Internet access to students is for educational benefit only.

21. Before a student is allowed to access the Internet, an Authorized Use Policy must be signed by both the student and parent and will be kept on site. Students and parents will sign the AUP each time a student enrolls at a new campus.

22. Standard e-mail exchange accounts will be issued to District employees. Secondary students in grades 6-12 will be assigned a student email account provided by the current district approved provider.Elementary students will not be issued individual e-mail accounts but may be provided access to e-mail through a classroom account.

23. Users will not post personal contact information about themselves or others.

24. Users who receive files that contain personal information about employees or students either by intentional or unintentional means must maintain all privacy regulations as stated in this policy.They may not copy, forward or distribute such information.

25. Users are not allowed to intentionally transmit or receive obscene, pornographic or inappropriately suggestive content or language in the form of images, files or multimedia files types through any synchronous or asynchronous communication device or software used in the Little Rock School District.

26. All users should observe network etiquette. Users are expected to be polite and use appropriate language. Using vulgar or profane language is not appropriate. Engaging in flaming or spamming is not appropriate. Students are prohibited from using chat rooms and instant messenger services unless authorized for educational purposes. Participation in cyber bullying (original,secondary, or distributed) is prohibited.

27. Use of the system to access, store or distribute obscene, pornographic, or inappropriately suggestive material is prohibited.

28. Use of the LRSD networks and computers to access, store, or distribute materials or sites that are considered racially derogatory, homophobic or "hate sites" is strictly prohibited.

29. Students are to immediately report any inappropriate material they access to a teacher or other staff person. Students are not to share inappropriate materials or their sources with other students.

30. Teachers and staff should report any inappropriate, illegal behavior or misuse of district devices, systems or networks immediately to their supervisors.

Supervision of the Computer Network

31. Coordination of the District computer network is under the supervision of the Superintendent or designee. At the building level, the principal or designee will be responsible for coordination of activities related to the network.

32. Monitoring for proper use of email, Internet searches, chat rooms and other forms of social media, and/or violations of any type are performed through, but not limited to, Gaggle, LanSchool, teacher observation, filtering and network management software.

33. The principal or designee will establish a system that ensures that all employees,authorized users, vendors and students receive instruction in District policies that address computer systems and networks.The principal or designee will also establish a process for supervision of students using the system and will maintain user and account agreements.

34. The principal or designee will establish a process for reviewing these regulations with employees annually. The Employee Use Agreement must be signed annually by all employees. The students will sign the Acceptable Use Policy, once in Elementary, Middle and Senior High. Parent's signature will be required even when student transfers to another school.

Administrative Access to Programs

35. Due to increased demand of data reporting in the district, it becomes necessary to allow certain personnel administrative access to programs. These programs include, but are not limited to GradeQuick/Edline, Site Reporter, AS400 (I-Series)and Parent Link. The access holds an incredible amount of responsibility due to the privacy issues of student records outlined in FERPA.Administrative access to programs should be determined and documented using the following procedures:

- Identify the school personnel that needs access
- Document purpose of the access
- Document written approval by supervisor
- Length of time access should be granted
- Yearly review of users who have access to programs

District Maintained Content Management Site and Pages

36. Edline Pages and School Sites: Schools maintaining Edline pages and/or school websites must remain consistent with the purpose of informing parents and the community of school related news and information, student achievement and links to other pertinent educational resources.

37. Social Networks: All users must maintains high level of respect when using social media as a district employee or as students. Educators should follow the Arkansas Department of Education Rules Governing the Code of Ethics for Arkansas Educators when dealing with students in online activities. See Standards of Professional Conduct 5.01.

Penalties for Non-Permitted Activities

38. Any user who violates this policy and accompanying regulations is subject to loss of computer, phone, and network privileges as well as other District disciplinary actions as outlined in the LRSD Rights and Responsibilities Handbook.

This policy may be revised at any time by a two-thirds vote of the LRSD School Board of Directors or as state and federal law dictates.

Date: March 23, 2006

Revised:November 28, 2011

Approved: December 15, 2011 (Appendix E)

Little Rock School District

Authorized Use of Computer Networks Policy

Student Use Agreement

Student Section

School

Student NameGrade

I have read the District Authorized Use of Computer Networks Policy. I agree to follow the rules contained in this policy. I understand that if I violate the rules my computer privileges can be terminated and I may face other disciplinary measures.

Student SignatureDate

Parent or Guardian Section

I have read the District Authorized Use of Computer Networks Policy.

I hereby release the District, its Board of Directors, staff, employees, and any institutions with which it is affiliated,from any and all claims and damages of any nature arising from my child's use of, or inability to use, the District computer network. This includes, but is not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

I will instruct my child regarding any additional restrictions I wish to be followed in addition to those outlined in these regulations. I will emphasize to my child the importance of following the rules for personal safety.

I give permission for my child to participate in the District's electronic communications system and certify that the information contained on this form is correct.

I do not give permission for my child to participate in the District's electronic communications system.

Parent Signature Date

Print Parent Name

HomeAddress Phone

Parent's e-mail address

Little Rock School District

Authorized Use of Computer Networks Policy

Employee Use Agreement

School or Department

EmployeeNam e

Employee access to the District's computer network is primarily to be used as a tool in the performance of the employee's job.

****

I have read the District Authorized Use of Computer Networks Policy. I agree to follow the rules contained in this policy. I understand that if I violate the rules my account can be terminated and I may face other disciplinary action.

Employee Signature Date