625 Irving St.
Forrest City, AR 72335

Telephone: 870-633-1485

Fax: 870-633-1415

Forrest City Public School District
Acceptable Computing Device and Network Use Policy

Technology users' responsibilities go beyond general care of computers, iPads, other computing devices, and the computer room. The Forrest City School District's policy addresses the acceptable use of technology hardware, software, networks, and the Internet.

District Responsibility Regarding the Computing Network

A. The Forrest City Public School District is responsible for:

1. Management of the network--the wires and devices (e.g., servers, routers, switches) that comprise the Network.
2. Setting standards for the hardware and software that can be used in the network.
3. Maintaining and repairing equipment purchased by the district for use in the network.
4. Providing training to users in the use of all district-supported hardware and software
5. Assigning and revoking privileges regarding use of the network
6. Defining the rights and responsibilities of users and enforcing acceptable use standards

B. The Forrest City School District will provide users with hardware, software, and electronic resources that support the mission of the school district. However, computing resources all come at a cost. The district will provide services at a level that the School Board determines meets the mission of the district to the best of its ability within the constraints of financial resources.

Unless otherwise specified, the following regulations will apply equally to students, employees, volunteers, and contractors employed by the Forrest City School District. Employees, volunteers, and contractors may have additional obligations owing to the nature of their positions and/or access privileges.

All individuals with access to Forrest City School District technology and computer networks will:

1. Respect the rights and property of others and will properly access files, data, or information of others.
2. Observe Forrest City School District standards of conduct as stated in the handbook.
3. Utilize the computers, mobile devices, network, Internet, and other technologies only for purposes in support of the district's stated education goals or for legitimate school district business.
4. Be responsible for taking precautions to prevent loss or damage to equipment and data.
5. Install and use software on the district's computing devices only in accordance with Software Policy and Procedure Guidelines.

Interpretation, application, and modification of this use policy are within the sole discretion of the Forrest City School District. Any questions or issues regarding this policy should be directed to the building or district administration, or the network administrator(s).

Internet Safety Policy

The Forrest City School District is compliant with the **CHILDREN'S INTERNET PROTECTION ACT (CIPA) (Pub.L.106-554)** through the use of internet filtering by the State of Arkansas's Division of Information Services, and through the use of adult monitoring and supervision of students who use district computers, iPads, and other computing devices. The Forrest City School District is compliant with the **Neighborhood Children's Internet Protection Act (NCIPA)** by providing an Internet Safety Policy, and the District enforces the requirements of these policies.

The Forrest City School District strictly forbids the access of inappropriate or harmful material, as defined in **Pub.L.**

106-554, on the internet and World Wide Web from any district owned computer, other computing device, or district owned network connection. This includes all employees of the district, as well as minors. The Forrest City School District further forbids students' direct electronic communications through the use of district or other forms of email, chat rooms, and/or any other form of direct electronic communication. Any exceptions to direct electronic communication must be with prior written approval of the Supervisor of Technology, and under the continuous direct supervision of a certified teacher, librarian, counselor or administrator with knowledge and approval by each site's building supervisor.

The Forrest City School District strictly forbids the unauthorized disclosure, use, and dissemination of personal identification information of minors. Written permission by the legal parent or guardian must be on file in the school or district office prior to the disclosure, use, or dissemination of personal identification information of minors. This permission includes the publication or display of photographs on district web sites. Pictures with no personal identification information as part of a larger graphic presentation are allowed.

The Forrest City School District strictly forbids the unauthorized access, including so-called hacking and other unlawful activities, by any person using district owned equipment or district connection points to the Internet. The Forrest City School District educates minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms. Each school incorporates strategies appropriate for the age level of the students to address this. Included is emphasized training about cyberbullying and the responses that the district will take to deal with such issues.

Electronic Network Use Rules

Every user (which includes, but is not limited to students, employees, volunteers, and contractors employed by the district) has the responsibility to respect and protect the rights of every user in our community and on the Internet. School district account holders are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use, and the laws of the state and the United States. Students will be provided with a school atmosphere and procedures of student control/discipline that will assure a suitable learning environment, and students will learn to act as responsible and productive citizens with respect for civil rights and the role of the individual in a democracy.

Computer/Computing Device Use Rules (NOTE: The use of the term computer refers not only to desktop computers, but also to notebook computers, iPads, iPods, NOOK, Kindle, iPhones or other smartphone, and any other Internet accessible computing device, whether school owned or personal device.)

- Food and drink are not allowed in any computer area.
- No software is to be downloaded, stored, or installed on any computer or other computing device or in any computer account without approval from the Technology Department.
- Pirated software (warez) and MP3s are not to be downloaded or stored on any computer, computing device, or in any user's account.
- Modification or removal of digital electronic files that are not your own is not allowed.
- All copyright laws are to be observed. Copyrighted material is not to be placed in the system without the author's permission (Copyright Law of 1994; Digital Millennium Act of 1998).
- You are not to move or disconnect any computer or peripheral device or piece/part of any equipment.
- Contact a supervisor or teacher concerning problems with any of the equipment.
- Appropriate behavior and common courtesy are expected at all times.
- You should not send anything to a printer unless you absolutely need a hard copy of the information; do not print web sites without knowing exactly how many pages will be printed; do not print multiple copies of any document without specific permission.
- Do not read other users' electronic mail or files, nor attempt to delete, copy, modify, or forge others' files or e-mail.
- Do not interfere with others' ability to send or receive e-mail.
- Do not disseminate personal identification information about yourself or others, including personal address, social security number, and phone number.
- Do not use the network in such a way that would disrupt the use of the network by other users.

- Do not use the system to encourage the use of drugs, alcohol, tobacco, or any illegal/inappropriate activities .
- Passwords must be strong, kept confidential and not shared with anyone else. A strong password is at least 8 characters in length with a mix of lower case(abc…z) and upper case(ABC…Z)letters, symbols(#&@...) and numerals(1234…).
- Users should not allow any other person access to any device logged in under their own account.
- Only Teacher approved downloads such as elements to be used in presentations are allowed. Media must be available within the scope of copyright laws and checked for viruses prior to any use, using the district's antivirus software supervised by the teacher.
- Do not leave portable devices unattended to prevent theft.
- All videos must be approved for viewing by the building administrator. Any video checked out of the library is pre-approved.
- Network printers should be used responsibly to prevent waste and/or abuse.

Using the network is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. Unacceptable conduct includes, but is not limited to, the following:

- Using the network for any illegal activity, including violation of copyright or other contracts.
- Using the network for financial or commercial gain.
- Using the network while access privileges are revoked or suspended.
- Degrading or disrupting equipment or system performance.
- Vandalizing the data of another user.
- Theft or plagiarism of data.
- Wastefully using finite resources.
- Unauthorized downloading of software.
- Gaining unauthorized access to resources or entities.
- Willfully and knowingly accessing or attempting to access pornographic or other inappropriate sites.
- Invading the privacy of individuals.
- Using an account owned by another user without authorization.
- Posting personal communications without the author's consent.
- Posting anonymous messages.
- Placing of unlawful or unlicensed information on a system.
- Using abusive or otherwise objectionable language in either public or private message.
- Sending of messages that are likely to result in the loss of recipients' work or systems.
- Sending of chain letters or broadcast messages to lists or individuals, or any other type of use that would cause congestion of the networks or otherwise interfere with the work of others.
- Playing games on the internet that are not designated and approved, with lesson plans and educational goals to support their use.
- Student use of a teacher computer, unless correctly logged in and supervised by the teacher.
- Using the computer, projector, and smartboard to show any movies that do not have an educational purpose supported by lesson plans and identified standards and benchmarks.

Acceptable Posting: The Forrest City School District provides a public Internet presence to share information with the community. Staff members are allowed to use these district provided resources and are responsible for monitoring and reviewing all content created by students. Students are not allowed to directly publish information to the public Internet via the school district network. Staff members agree not to publicly publish through the school district site any information that 1) violates copyright laws or property rights, 2) discloses student personal information, 3) discloses student names with photographic depictions, 4) contains deliberately false or misleading statements regarding the school district, 5) are illegal, 6) are deliberately offensive, threatening, or libelous, or 7) are pornographic or otherwise obscene.
False Entry/Alterations: No student, volunteer, or school/district employee will make any false entry or alteration of any document, (either paper or electronic) used or intended to be used in connection with the operation of the Forrest City School District nor any school in the district, nor will any student open or alter official school documents or private documents, either paper or electronic.
Data Security: The District assumes no responsibility or liability if documents stored on school equipment are lost or

damaged, nor will the district be responsible for security violations beyond the appropriate punishment of those persons involved in such violations.

Controlled Access to the Internet: Internet access is provided strictly for use consistent with the district's educational and business goals. It is the practice of the Forrest City School District to protect staff and students from obscene, pornographic, and other inappropriate material available on the Internet by monitoring Internet access and by using mechanisms such as content filters and firewalls in accordance with the Children's Internet Protection Act.(CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA). Students are not allowed to access the Internet without staff supervision and are required to connect to the web through a content filter. Attempts to access inappropriate material are logged. Deliberate attempts to access obscene or inappropriate materials by any user will result in disciplinary action by school district administration. The school district may provide direct communication systems such as e-mail or chat rooms for student use, which will be either filtered for content, closed (in-district only), or both. To provide student safety and security, the use of Internet direct communication systems is allowed only under direct staff supervision. Web-based direct communication systems pass through a content filter.

Unlawful and Unauthorized Activities: The Forrest City School District does not tolerate the use of the network for illegal activity, including electronic crimes such as unauthorized access, deliberate use of malicious code such as viruses, and deliberate attacks on systems ("hacking"). Cyber-bullying will not be tolerated by the Forrest City School District. These activities will result in disciplinary action by school district administration. In addition, if requested by any law enforcement agency, the technology department will cooperate completely to identify those who carry out illegal activities, document proof of such activities, and testify in court.

Vandalism - Vandalism will result in cancellation of privileges as well as other sanctions or disciplinary action. Vandalism is defined as any malicious attempt to harm, modify, or destroy computer hardware, data of another user, Internet, or any of the other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses.

Network Etiquette

- Be polite. Do not get abusive in your messages to others.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the network.
- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
- Exercise caution with personally identifiable information.
- Do not reveal personal information of others. Any student receiving unsolicited requests for personal information will immediately report that to the supervising teacher. That teacher will report this incident to appropriate authorities.
- Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to authorities.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- Information accessible via the network and Internet should be assumed to be private property and possibly copyrighted.
- Do not take part in any form of chain letters, mass mailings, or pyramid schemes that ask for forwarding a message to others. Many people find these very disconcerting and intrusive.

Enforcement

Violation of the rules set forth by school district policy may result in disciplinary action by school district administration. The Director of Technology is empowered to suspend some or all privileges associated with computer/computing device use in cases of misuse or threat to the integrity of information technology resources. Disciplinary action for misuse by students may include, but is not limited to, suspension from school, removal from classes requiring computer use, loss of computer use privileges, and, if deemed appropriate, criminal prosecution. Disciplinary action for misuse by employees and other users may include, but is not limited to, formal reprimand, probation, termination, and, if deemed appropriate, criminal prosecution. School district administration and the technology department will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final. Before any permanent action is taken against a user, the user

will be advised of the basis for the proposed action and given an opportunity to respond. The specific disciplinary action for each case will be at the sole discretion of school district administration and may vary depending on the severity of the infraction.

Security

Security on any computing device is a high priority. Do not use another individual's account. Attempts to log onto the network with another person's identification without permission may result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computing systems may be denied access to the computers and network. If you feel you can identify a security problem on the network, you must notify an administrator.

Policy Agreement

The Forrest City School District will uphold laws pertaining to the use of information technology equipment and the information contained therein and/or generated by its use. Anyone found to be violating such laws would be subject to suit for civil damages as well as prosecution to the full extent of the law.

There is a need for full disclosure and understanding for the partnership between parents, children, and the school district in regard to technology and its use. A Computing Device and Network Use Agreement has been created to inform and provide knowledge, ensuring that all parties understand the areas of responsibility identified. Each child will need to have an agreement form signed and on file before the student will be allowed to use the computers or other computing device.

Software Policy and Procedures

Purpose: The Forrest City School District licenses the use of computer software from a variety of third parties. The software developer normally copyrights such software. Unless expressly authorized to do so, the Forrest City School District has no right to make copies of the software except for backup or archival purposes. The purpose of this policy is to prevent copyright infringement and to protect the integrity of the Forrest City School District's computing environment from viruses and similar threats. The term software herein also refers to apps for iPads and other computing devices.

Policy and Procedures Guidelines: It is the policy of Forrest City School District to respect all computer software and application (apps) copyrights and to adhere to the terms of all software licenses to which the district is a party. The Director of Technology is charged with the responsibility of monitoring these guidelines and assuring compliance. Forrest City School District employees may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless the Forrest City School District is expressly authorized to do so by agreement with the licenser. Unauthorized duplication of software may subject employees, students, and/or the district to both civil and criminal penalties under the United States Copyright Act. Employees may not give standalone software to any other employee or any software to non-employees including parents, contractors, students, and others. Forrest City School District employees and students may use software on local area networks or on multiple machines only in accordance with applicable license agreements.

Acquisition of Stand-Alone Software: To purchase and utilize software within the Forrest City School District, employees must obtain the approval of their supervisor or Director of Technology. All software utilized by employees of the Forrest City School District must be registered with the Director of Technology. Software acquisition channels are restricted to ensure that the Forrest City School District has a complete record of all software that has been purchased for district computers/computing devices and can register, support, track, and upgrade such software accordingly. All software will be subject to review and approval by the Technology Department.

Acquisition of District-Wide Software: In order to facilitate the selection and implementation of software for use district-wide, a committee of district staff will be utilized to analyze and evaluate software packages. The committee participants will include staff members from each affected location and be led by the Director of Technology, as to ensure that the selection best meets the needs of the district. At all stages, factors such as user reaction, effect on workload and efficiency for users and support personnel, and resources required should be considered.

Registration of Software: The district will register every software package. When a staff member acquires new software for use on district computers, he/she must inform the school media specialist. The staff member should provide a copy of the registration to the school media specialists. Software must be registered in the name of the district and department/school in which it will be used. Because of personnel turnover, software should never be registered in the name of the individual user. The school media specialist shall maintain a register of all of the district's software and shall keep a library of software licenses. The register will contain:

- the title and publisher of all software;
- the date and source of software acquisition;
- the location of each installation;
- the name of the authorized user;
- the existence and location of media ;
- the software product's serial number.

Storage and Security: The school media specialist shall be in charge of storing all school software in secured storage areas, if feasible. The Technology Department is in charge of all District Software. By ensuring secure storage of original media, the risk of software theft and unauthorized duplication of software is minimized.

Installation of Software: After the registration requirements above have been met, the software may either be installed by the Technology Department or qualified individuals with the Technology Department's permission. No software shall be installed on district devices without approval of the Director of Technology. Teachers who bring in data media from home are responsible to ensure that his or her media are free from viruses. District virus protection software should be used to examine these media before they are used in a district computer. These standards are to ensure that the district does not violate copyright laws or infect computer systems with viruses. A student shall not install computer software or tamper in any way with district software at any time. No student shall bring in media from home, unless under direct supervision of the teacher for which the contents of the media are intended and only with approved software. It is the responsibility of teachers and other faculty members to constantly monitor student use of computers/computing devices and review all policies and procedures with the students regarding the acceptable use of technology.

Documentation: Original manuals, tutorials, and other user-oriented documentation will be made available, whenever possible, to assist the software users. The district's trainers will also continue to provide in-service for teachers in the use of appropriate software.

Home Computers: The Forrest City School District's computers are district assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on district machines. Generally, district owned software cannot be taken home and loaded on an employee's computer if it also resides on the district's computer. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. Before taking any software home, please check with the Director of Technology and follow the sign-out and sign-in procedures.

Software Audits: The Director of Technology will conduct random audits of all district computing devices to ensure that the district is in compliance with all software licenses. During these random audits the district will search for inappropriate software and eliminate any that is found.

Software Log: A software log will be maintained of all software owned or used by the district. After the audit has been completed, the software log will be used to list all old and newly acquired software.

Penalties and Reprimands: Anyone who violates this policy will be referred to district administration for possible disciplinary action.

Hardware Policy and Procedures

Property Rights: The Forrest City School District has the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment purchased or received by way of grant by a school or the district will be the property of the district. The district or school will determine its use. In accordance with grant specifications, neither employees, volunteers, nor students in the school have ownership rights to any equipment loaned to them by the school. Use of school equipment and software for private or personal business is strictly prohibited and will subject the violator to disciplinary action.

No person will have exclusive use of school equipment unless authorized by district administration.

Acquisition: Any new acquisition of hardware is the responsibility of the Technology Department. Purchases may be made from vendors identified on the approved State Contracts lists, the State TIPS/TAPS list, or by quotes/bids. Any staff who wishes to supplement hardware with additional hardware must receive written permission from the Director of Technology. Any installation of hardware must be done by the Technology Department or its designee.

Network Attached Devices: Use of network attached devices, including, but not limited to, computers, printers, and handheld devices (i.e. iPads, iPhones, iPods, other smartphones, etc.), must be approved by the Technology Department to ensure the compatibility, stability, and security of the district network.

Wireless Devices: Use of wireless equipment must be approved by the Technology Department to ensure the compatibility, stability, and security of the district network. To ensure that security standards are met, wireless devices will not be used until configured appropriately by district technology personnel. Any wireless device deemed to be a security liability will not be allowed. Random scans for rogue wireless devices may be performed by district technology personnel.

Enforcement: The District and all schools in the district will rigorously uphold laws pertaining to the use of technology equipment and the information contained in them and/or generated by its use. Anyone found to be violating such laws would be subject to suit for civil damages as well as prosecution by the school to the full extent of the law.

Warranties/Indemnification

The District believes that the benefits to educators and students from access to the Internet (in the form of information resources and opportunities for collaboration) far exceed any disadvantages of access. Ultimately, parent(s) and guardian(s) of minors are responsible for their child's behavior, and this includes use of the Internet.

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computing networks and the Internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer 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, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the Internet.
The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

Legal Reference: Children's Internet Protection Act, P.L. 106-55
20 U.S.C. § 6801, et seq.
47 U.S.C. § 254(h) and (1)

Wireless Security Policy

Forrest City School District uses an enterprise wireless solution to provide management and an additional level of security to the wireless network. All access points are located in physically secure locations. Access to wireless management is limited and requires strong authentication. To minimize potential exposure and risk of district data, including but not limited to loss or corruption of sensitive, confidential or financial data, Forrest City School District has the following security measures in place for Wireless Security:

- To prevent unauthorized access, the district requires faculty, staff and students to use strong passwords. Broadcast SSIDs require web portal authentication using Active Directory credentials. MAC address filtering is in effect. All default passwords have been changed. On occasion, when guest access is required, the guest network password is given out. Guest access is routed on a separate VLAN which allows Internet access but no access to the network. The guest password is changed regularly.
- Access to wireless management is limited to the technology department personnel using specified accounts with strong passwords.
- Updates are configured to keep access point software patched. The network administrator manually checks for updates to ensure that updates are installing correctly.
- This policy is included in the Acceptable Use Policy that all employees sign at the beginning of each school year.
- The network administrator checks for rogue devices at least once per month, and unidentified devices are denied access.
- All district buildings have secure access requiring a physical key. Access control is limited based on employee position. Wireless access points are located in physically secure locations.
- At the end user level, all district owned machines have anti-virus and anti-malware utilities installed to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- A warning banner is displayed on each district owned machine informing users of the acceptable use of the network and possibility of monitoring.
- At the wireless access point, firewall rules and application rules, as well as an encrypted password for the SSID are configured to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- At the district level, all devices are behind a firewall and a content filter that applies real-time monitoring which is used to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- As an ongoing effort, the district will continue to follow the Best Practices Statement from DIS (http://www.dis.arkansas.gov/policiesStandards/Documents/BP-70-010_wireless_best_practices.pdf).

625 Irving St.
Forrest City, AR 72335

Telephone: 870-633-1485
Fax: 870-633-1415

Forrest City School District
Computing Device and Network Use Agreement

School district computer and Internet accessible device users are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use, and the laws of the state and the United States.

The computers, computing devices, and network are provided for furthering the District's stated educational goals only, and they are to be used by authorized individuals only. Individuals using these systems are subject to having all activities on these systems monitored by system or security personnel. Anyone using these systems expressly consents to such monitoring.

It is possible for all users of the Internet, including your child, to access information that is intended for adults. Although the District has taken reasonable steps to ensure that the Internet connection is used only for purposes consistent with the curriculum and that inappropriate sites (as defined by the Children's Internet Protection Act) are filtered, the district or school cannot entirely prevent the availability of inappropriate material elsewhere on the Internet.

It is possible that a determined user may make use of computer resources for inappropriate purposes. Deliberate misuse of the computer network or the Internet may result in disciplinary action as outlined in the Computing Device and Network Use Policy.

I,_____ and _____
Parent Name (please print) Student Name (please print)

have read the Computing Device and Network Use Policy, understand it, and agree to adhere to the principles and procedures detailed within. We understand and accept the conditions stated above and release from any liability the Forrest City School District, its subcontractors, and employees.

I understand that my child is expected to use good judgment and follow the guidelines of the Computing Device and Network Use Policy. Furthermore, I have discussed the information contained in the Computing Device and Network Use Policy with my child. Should my child breach the policy guidelines, I understand that my child may lose privileges on the Forrest City School District computer network and/or be subject to other disciplinary action.

_____ _____
Parent Signature Student Signature

_____
Date

625 Irving St.
Forrest City, AR 72335

Telephone: 870-633-1485
Fax 870-633-1415

Forrest City School District
Computing Device and Network Use Agreement

School district computer and Internet accessible device users are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use, and the laws of the state and the United States.

The computers, computing devices, and network are provided for furthering the District's stated educational goals only, and they are to be used by authorized individuals only. Individuals using these systems are subject to having all activities on these systems monitored by system or security personnel. Anyone using these systems expressly consents to such monitoring.

It is possible for all users of the Internet to access information that is intended for adults. Although the District has taken reasonable steps to ensure that the Internet connection is used only for purposes consistent with the curriculum and that inappropriate sites (as defined by the Children's Internet Protection Act) are filtered, the district or school cannot entirely prevent the availability of inappropriate material elsewhere on the Internet.

It is possible that a determined user may make use of computer resources for inappropriate purposes. Deliberate misuse of the computer network or the Internet may result in disciplinary action as outlined in the Computing Device and Network Use Policy.

I,_____ at _____
Staff Member (please print) Location (please print)

have read the Computing Device and Network Use Policy, understand it, and agree to adhere to the principles and procedures detailed within. I understand and accept the conditions stated above and release from any liability the Forrest City School District, its subcontractors, and employees. I understand that as part of classroom management I will supervise any student use of computers/computing devices while said students are under my charge or control.

I understand that I am expected to use good judgment and follow the guidelines of the Computing Device and Network Use Policy. Should I breach the policy guidelines, I understand that I may lose privileges on the Forrest City School District computer network and/or be subject to other disciplinary action.

_____ _____
Signature Position

_____
Date