

## PERSONNEL INTERNET ACCEPTABLE USE POLICY

Name (Please Print)

---

School \_\_\_\_\_ Date \_\_\_\_\_

The Hot Springs School District agrees to allow the employee identified above ("Employee") to use the district's technology to access the Internet under the following terms and conditions:

### Conditional Privilege

The use of Hot Springs School District's technology is a privilege, not a right. Staff must supervise students' use of technology at all times. The Employee agrees that in using the District's Internet access he/she will obey all federal and state laws and regulations. Internet access is provided as an aid to employees to enable them to better perform their job responsibilities. Under no circumstances shall an Employee's use of the District's Internet access interfere with, or detract from, the performance of his/her job-related duties

### Access Statement

All users must sign and return an Acceptable Use Policy Statement before being allowed to use any of the District's technology. The Acceptable Use Agreement will stay in effect as long as the staff member is employed in the District.

### Social Networking

1. Prior to establishing professional social media accounts, a written explanation of the purpose of the account should be provided to district level administrators for approval.
2. If the District approves the use of professional social media accounts, parents/guardians should be notified of the purpose and provided an opportunity to "opt out."
3. E-mail and/or social media tools and accounts should be kept separate. Professional accounts should be created and maintained separately for student and/or parent interaction and communications.
4. Personal accounts should be for personal use only. School personnel should not add students and/or parents as "friends" or "associates" to personal accounts.
5. Use of social media during business/school hours should be on professional accounts and for professional or educational use only.
6. Digital correspondence between school personnel, students, or parents should be limited to professional and educational purposes only, and be conducted at appropriate times.
7. Images, audio, or videos of any school activities or students should not be digitally transmitted or streamed without prior written parental consent and/or must adhere to local district policies.

### Acceptable Uses

1. Classroom assignments requiring Internet research
2. Career development activities
3. School Sponsored email
4. Approved use of Web Applications for instructional use.
5. Educational research

### Unacceptable Uses

1. Use of swear words, vulgarities, or any other inappropriate language in any messages or web pages.
2. Accessing any site on the Internet that is not consistent with the educational objectives of the District.
3. Participating in "Cyber Bullying" such as personal attacks and/or threats on/against anyone.
4. Using the network/Internet for any illegal activity, including violation of copyright laws or other contracts or transmitting any material in violation of any federal, state or local law

5. Sending, receiving, viewing, or downloading any illegal material
6. Unauthorized downloading or installing of software to any District electronic devices or any electronic device, such as an mp3 player
7. Using the computer system for private financial or commercial gain
8. Wastefully using resources, such as bandwidth, file space, paper, and ink/toner
9. Gaining unauthorized access to resources or entities (hacking)
10. Using the computer system for commercial or private advertising
11. Submitting, posting, publishing or displaying any obscene, profane, threatening, illegal, or other inappropriate material
12. Using the computer system while access privileges are suspended or revoked
13. Vandalizing the computer system, including, but not limited to, modifying or destroying any other peripheral equipment, or destroying data by creating or spreading viruses and/or by any other means
14. Forging, intercepting, or interfering with electronic mail messages
15. Accessing or attempting to access instant messages, non-educational chat rooms, forums that are not school-related, private e-mail, message boards, blogs or wikis that are not school-related.
16. Failing to respect the District's computer system's resource limits
17. Using the computer system to disrupt others
18. Reading, modifying or deleting data owned by others, except as otherwise provided in this policy.
19. Bypassing or attempting to bypass the District's Internet filter or other security measures through means such as, but not limited to, online proxies, bootable media, IP spoofing, etc.
20. Intentionally damaging the system, information belonging to others, or system resources, or allowing others to misuse system resources.
21. Attempting to vandalize computers, networks, printers, or other associated equipment or system resources. Alteration or vandalism includes, but not limited to, removal of parts, intentional destruction of equipment, attempting to degrade or disrupt system performance, or attempting to make system resources unusable.
22. Users shall not relocate or remove technology equipment (hardware or software) from its location without permission from the HSSD Technology Department.
23. Users shall not use system resources to distribute or provide personal information or addresses that others may use inappropriately.
24. Users should be aware that electronic mail (e-mail) and all other files stored on the District's network are the property of Hot Springs School District.
25. Users should not send any messages or create any files that they would not want to be made public. Space restrictions will be implemented according to District guidelines.
26. Users shall maintain a strong password on District computers, email system, and any other network logins at all times.
27. Teachers are strictly prohibited from allowing students to use their logins/credentials on any device on the district's network or to provide any other unauthorized access at any time

### **Violations Consequences**

1st Offense: Warning and documentation in personnel file

2nd Offense: Disciplinary action and formal improvement plan

3rd Offense: Possible suspension and/or recommendation for non-renewal or termination

### **Internet Access**

1. All Internet usage is monitored, and users should expect that their use may be reviewed at any time by the principal or superintendent or his/her designee.

2. Staff will be issued an e-mail account for educational use.

### **Responsibility**

Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should users provide their passwords to anyone else.

**No Expectation of Privacy**

Users should not expect privacy in the contents of their personal files stored on the District's network; they must realize that any information stored electronically on school-owned equipment is subject to Arkansas' Freedom of Information Act. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice, any and all usage of the computer network and/or internet usage.

**Liability Disclaimer**

Liability for debts: Staff shall be liable for any and all costs (debts) incurred through their use of the District's computers or the Internet including penalties for copyright violations.

**Staff Agreement**

The acceptable and unacceptable uses of the District's equipment, network and Internet access are described in this "Acceptable Use Agreement". By signing this agreement, I acknowledge that I have read, understand and agree to abide by the provisions of the attached Acceptable Use Policy. I realize that all the rules of conduct described in this District's AUP, policies, procedures, and handbooks apply when I am using the District's network.

**Staff Name:** \_\_\_\_\_ **Email:** \_\_\_\_\_ **(Print)**

**Staff Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

Adopted by Board of Education  
January 17, 2012