



**Pine Bluff
School District
Technology Services**

Excellence All Day Every Day

512 Pine St. P.O. Box 7678 Pine Bluff, AR 71611 870.543.4348

ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE COMPUTER NETWORK OF THE PINE BLUFF SCHOOL DISTRICT

The Pine Bluff School District is pleased to make available to students access to our computer network systems within the District and to the Internet; The world-wide Web Network that provides various means of accessing significant educational materials and opportunities.

In order for the Pine Bluff School District to be able to continue to make its Computer Network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's Misuse of the network's Internet access wired or wireless may jeopardize the ability of all students to enjoy such access. While the schools' teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy of the Pine Bluff School District and the Department of Information Systems that provides Internet access to the District. Upon reviewing, signing, and returning this policy as the students have been directed, each student will be given the opportunity to enjoy Internet access at school and is agreeing to follow the policy. If a student is under 18 years of age, he or she must have his or her parent or guardians read and sign the policy. The Pine Bluff School District cannot provide access to any student who, if 18 or older, fails to sign and submit the policy to the school as directed or, if under 18, does not return the policy as directed with the signatures of the student and his/her parents or guardians.

Listed below are the provisions of your agreement regarding computer network and Internet use. If you have any questions about these provisions, you should contact the principal of your school. If any user violates this policy, the student's access will be denied, if not already provided, or withdrawn; and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing this policy, you are agreeing not only to follow the rules in this policy but also to report any misuse of the network to the person designated by the school for such reporting or to the principal of the school if you do not know this designated person misuse means any violation of this policy or any other use that is not included in the policy, but has the effect of harming another or his or her property.

II TERM OF THE PERMITTED USE

A student who submits to the school, as directed a properly signed policy and follows the policy to which she or he has agreed will have computer network and internet access during the course of the school year only. Students will be asked to sign a new policy each year during which they are students in the Pine Bluff School District before they are given an access account.

III ACCEPTABLE USES

A. Educational Purposes Only. The Pine Bluff School District is providing access to its computer networks and the Internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide if a use is appropriate.

B. Unacceptable Uses of Network

Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

1. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance, the possession or use of which is prohibited by the Pine Bluff School District's Student Discipline Policy; view, transmit, or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
2. Uses that cause harm to others or damage to their property. For example, don't engage in password sharing or defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "Trojan Horse," "time bomb," or other harmful form of pro-gamming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
3. Uses that jeopardize the security of student access and of the computer Network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user.

4. Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

C. Netiquette. All users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
2. Avoid language and uses which may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other materials which are based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
3. Don't assume that a sender of e-mail is giving his or her permission for you to forward redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
4. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

IV. INTERNET SAFETY

- A. **General Warning; Individual Responsibility of Parents and Users.** All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guides to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the school.
- B. **Personal Safety.** Be safe. In using the computer network and Internet, do not reveal personal information such as your house address or telephone number. Do not use real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the computer network or internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.
- C. **“Hacking” and Other Illegal Activities.** It is a violation of this policy to use the school’s computer network or the Internet to gain unauthorized access to other computers or computer systems to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, and the distribution of obscene or pornographic materials or which violates any other applicable law or municipal ordinance is strictly prohibited.
- D. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purpose or approved education projects and activities.
- E. **Active Restriction Measures.** The school district, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The school district will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 U.S.C Section 254 (h)(7), as meaning any picture, image, graphic image file, or other visual depiction that was taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or perverted sexual acts, or a lewd exhibition of the genitals; taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

V. PRIVACY

Network and Internet access is provided as a tool for your education. The Pine Bluff School 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 Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the Pine Bluff School District and no user shall have any expectation of privacy regarding such materials.

VI. FAILURE TO FOLLOW POLICY

The user’s use of the computer network and Internet is a privilege, not a right. A user who violates this policy, shall at minimum, have his or her access to the computer network and Internet terminated, which the Pine Bluff School District may refuse to reinstate for the remainder of the student’s enrollment in the Pine Bluff School District. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The Pine Bluff School District may also take other disciplinary action in such circumstances.

VII. WARRANTIES/INDEMNIFICATION

The Pine Bluff School District makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user’s use or its computer networks or the Internet under this policy. By signing this policy, a user is taking full responsibility for his or her use, and the user who is 18 or older or, in case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the Pine Bluff School District, and all of their administrators, teachers, and staff harmless from any and all losses, costs, claims, or damages resulting from the 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) or guardian(s) agree to cooperate with the school in the event of the School’s initiating an investigation of a user’s use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the Pine Bluff School District’s network.

VIII. UPDATES

Users and, if appropriate, the user's parents/guardians may be asked from time to time to provide new or additional registration and account information or to sign a new policy to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardian) or such new policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the school to receive such information.

Wireless Network Access

Introduction:

This policy addresses the use of IEEE 802.11 wireless data networking protocols, commonly known as "Wi-Fi" or "wireless Ethernet." These protocols are used for connecting client devices to a data network through the use of over-the-air radio signals. The primary advantages of wireless networks are mobility and flexibility.

Definitions:

1. IEEE 802.11 is a set of wireless networking protocols and standards adopted by the Institute of Electrical and Electronics Engineers (IEEE). The 802 committee works on data networking standards. The 802.11 subcommittee works on the subset of wireless standards that are commonly known as Wi-Fi. These standards define the components and functions of devices in an 802.11 network. These standards also include add-on definitions such as 802.11a, 802.11b, 802.11g, 802.11i, 802.11b/g/n, and 802.11ac wireless standards, etc.
2. "Wi-Fi" is a term developed by the Wi-Fi Alliance to help identify devices that properly conform to the IEEE's 802.11 standards. The Wi-Fi Alliance was formed to help facilitate interoperability between wireless products from competing vendors.
3. Extended Service Set Identifier (ESSID or SSID) is the textual name of a wireless network. The SSID is used to identify the network and advertise its availability.
4. The phrase "*wireless service*" in this document refers to the Pine Bluff school Districts wireless data networking service provided by Technology Services.

Policy Statements:

1. Access to the wireless service will be restricted to current students, faculty, staff, and guests that have been authorized.
2. Students, faculty, and staff shall be authenticated with their student/faculty ID or password provided by the technology department or through the RADIUS server system. Guests will be provided a Guest ID or password from the Technology Department for authentication.
3. The wireless service shall protect authentication credentials through the use of data encryption.
4. Users of the wireless service are responsible for obtaining a device that meets the current implementation requirements if they are not using a school issued wireless device.
5. The text "PBSD_" is reserved for defining SSID's for the Pine Bluff School District wireless service.
6. Wireless equipment in PBSD owned or leased spaces that are not part of the Pine Bluff School District wireless service shall not include the text "PBSD_" in their SSID definitions.
7. PBSD Technology Services reserves the right to revoke wireless service authorization for an individual Hawk ID, Guest ID, or for any device that is disrupting the operation of the wireless service. Violation of the Pine Bluff School District Network policy or the Acceptable Use policy will result in revocation of authorization to use the wireless service.
8. PBSD faculty, staff, students and guests shall not install personal wireless networking equipment in The Pine Bluff School District's owned or leased spaces without written consent from Technology Services.

Implementation of the Policy

1. Responsibility for implementing this policy rests with District Administration; School based Administration and Technology Services. Technology Services is responsible for designing, configuring, installing, maintaining, and troubleshooting the Pine Bluff School Districts wireless service.
2. Technology Services will maintain a written description of the current wireless data networking implementation in the form of a service description. This will include device requirements for accessing the network, and information regarding procedures to obtain authorization for the deployment of user supplied wireless equipment.
3. Technology Services will utilize School District funds to provide a basic level of wireless service in classrooms, libraries, offices, and many common areas. Wireless service expansion will typically be funded by the district on an as needed basis.
4. Technology Services will provide a mechanism for procuring Guest ID's authorized to use the wireless service.
5. Technology Services is authorized to monitor/detect implementation of unauthorized wired or wireless devices. Technology services reserves the right to remove and/or disable wireless equipment that is in violation of this policy, and/or may disable any wired uplink data port associated with a device in violation of this policy.

Pine Bluff School District
STAFF INTERNET USE AGREEMENT

All Pine Bluff School District Staff who have directed access to the District's computer network and the Internet must read the policy and sign this form.

As an employee on staff with the Pine Bluff School District, I have read, understand, and agree with the terms of the District's Acceptable Use and Internet Safety policy for the student's access, as well as staff access, to the Pine Bluff School District's computer network and the Internet. I understand that access, is being provided to the students and staff for educational purposes only. However, I also understand that it is impossible for the School District to restrict access to all offensive and controversial materials and understand that it is my responsibility to abide by the policy. I am therefore signing this policy and agree to indemnify and hold harmless the appropriate school, the Pine Bluff School District, and the Department of Information Systems that provides the opportunity to the Pine Bluff School District for computer network and Internet access to such networks or violation of the foregoing policy. Further, I accept full responsibility for supervision of all children within the Pine Bluff School District who access the Internet form any computer on the District's network.

Employee Name (PRINT CLEARLY)

Home Phone

Employee Signature

Date

.....

ADOPTED: 3-2-2012

Acceptable Use and Internet Safety Policy

REVISED: 8-8-2012

Legal References: **Children’s Internet Protection Act of 2000 (H.R. 4577, P.L. 106-544)
Communications Act of 1934, as amended (47 U/S/C/ 254 (h),(1)
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C.
6801 et seq., Part F)**

STUDENT/PARENTS OR GUARDIAN’S AGREEMENT

Student’s Name

To be read and signed by parents or guardians of students who are under 18:

As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of the Pine Bluff School District’s Acceptable Use and Internet Safety Policy for the student’s access to the Pine Bluff School District’s computer network and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school district to restrict access to all offensive and controversial materials and understand my child’s ward’s responsibility for abiding by the policy. I am therefore signing this policy and agree to indemnify and hold harmless the appropriate school, the Pine Bluff School District, and the Department of Information Systems that provides the opportunity to the Pine Bluff School District for computer network and Internet access against all claims, damages, losses, an costs, of whatever kind, that may result from my child’s or ward’s use or his or her access to such networks or his or her violation of the foregoing policy. Further, I accept full responsibility for supervision of my child’s or ward’s use of his or her access account if and when such address is not in the school setting. I hereby give permission for my child or ward to use the building-approved account to access the Pine Bluff School District’s computer network and the Internet.

Parent or Guardian Name(s) (PRINT CLEARLY)

Home Phone

Parent or Guardian Signature(s)

Date

Student Signature(s)

Date

.....
Acceptable Use and Internet Safety Policy

ADOPTED: 3-2-2012

REVISED: 8-8-2012

Legal References: **Children’s Internet Protection Act of 2000 (H.R. 4577, P.L. 106-544)**
 Communications Act of 1934, as amended (47 U/S/C/ 254 (h),(1))
 Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)