

WELLPINIT SCHOOL DISTRICT

STAFF Appropriate Use Policy and Agreement

By signing this agreement, and as a condition for using the Wellpinit School District's computers, network and Internet access, I hereby signify that I understand and agree to abide by the following policies, which have been established by the Wellpinit School Board, in compliance with the Federal Children's Internet Protection Act

① Network Use

1. All use of the system must be in support of education and research and consistent with the mission of the district. District reserves the right to prioritize use and access to the system.
2. Any use of the system must be in conformity to state and federal law, K-20 Network policies, and school district policy. Use of the system for commercial solicitation is prohibited.
3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way. An exemption is made for modification of software by duly authorized network technicians.
5. Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on the system and/or damage the components of an entity on the network is prohibited.
6. Users are responsible for the appropriateness of the material they transmit over the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.
8. Student subscriptions to mailing lists, bulletin boards, chat groups, and commercial on-line services and other information services must be pre-approved by the superintendent or his designee. Students may not access bulletin boards or chat groups without the authorization of their teacher.
9. Students may not access personal email accounts from school unless permitted to do so by a teacher as part of an educational process, or unless written permission has been provided by the student's parent or guardian.
10. All these changes and other policies regarding the Internet shall be part of Appropriate Usage Policies (AUPs) to be signed by all Staff Members, and will be added to the Rules in the Student Handbook.

② Security

11. System logins or accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
12. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity on the K-20 Network.
13. Communications may not be encrypted so as to avoid security review. Encryption may be employed with the written permission of the district's Technology Director or Superintendent.
14. Users should change passwords regularly and avoid easily guessed passwords. Password changes will be pushed from the Technology Office.

③ Personal Information

15. Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian. All users should not disclose, use, or disseminate personal identification information regarding minors without authorization. Exemptions will be made for some of the content on the District's Web Site. The Web Site can display:

- Names, school phone numbers and school email addresses of all staff members, though not their home phone numbers
- Rosters of sports teams and listings of student awards
- Student work as assigned by a teacher
- Pictures taken of school activities – including all sports and field trips
- Our web site will post pictures identified with first names only – no full last names will be used.

If a parent objects to any display of student information, the District will provide a mechanism whereby the student in question will have no identifiable presence on the District's Web Site.

16. Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
17. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant Message services).

4 Filtering and Monitoring

18. No later than July 1, 2002, filtering software or services will be installed and used on all computers with access to the Internet, which will block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. When adults are using the Internet, materials which are obscene and child pornography must still be filtered or blocked.
Exceptions may be made for staff if the filtering software will not permit them access to sites that they need to access as part of their designated work.
19. Educational staff will, as part of their duties, monitor minors' use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, and restrict their access to materials harmful to minors.

5 General Use

20. Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files, and users should promptly disconnect videoconferences on completion.
21. No Staff Member shall have access to the K-20 Network without having received appropriate training, and having a signed Individual Appropriate Use Policy [AUP] Form on file with the district.
22. No student shall have access to the K-20 Network without having received appropriate training, and having an AUP Form signed by the student and a parent or legal guardian on file. It is the teachers' responsibility to ensure each child understand the AUP and has a signed AUP on file.
23. All school policies for students will be made part of the Student Handbook.
24. If a parent or guardian does not want their child to access the Internet, the District will provide a mechanism whereby the student will not access the Internet. The parent will also be informed of the ways in this will limit the educational opportunities for the student.
25. Nothing in these regulations is intended to preclude the supervised use of the network while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.
26. From time to time, the district will make a determination on whether specific uses of the K-20 Network are consistent with the regulations stated above. Under prescribed circumstances non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes the district reserves the right for authorized personnel to review network use and content. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity.
26. Violation of any of the conditions of use may be cause for disciplinary action.

By signing below, I indicate that I have read and understood the preceding points, and agree to abide by them as long as I am an employee of the Wellpinit School District.

Name of STAFF MEMBER _____

Signature _____

Date Signed _____