HOBBS MUNICIPAL SCHOOL DISTRICT
COMPUTING AND INTERNET ACCEPTABLE USE POLICY

A. **Purpose**
   1. The Hobbs Municipal School District is providing its employees and students ("users") with access to computing equipment, systems and local network functions such as District e-mail and the Internet.
   2. This access has a limited education purpose for students and is to facilitate employees' work productivity.

B. **Access rights and privileges.**
   1. The School District has the right to place reasonable restrictions on the use of equipment, resources and material students and employees access or post through the system. Students and employees are also expected to follow the rules set forth in the District's rules and regulations governing conduct, disciplinary code, and the law in their use of the District's equipment and network. This access has not been established as a public access service or a public forum. All access and rights are privileges granted by the District, and users should expect no privacy rights.
   2. All District employees and students will have access to the Internet through the District's private network. Parents may specifically request that their children not be provided such access by notifying the District in writing.
   3. No student will be given or have access to District-provided e-mail.
   4. Guests/contractors are not automatically eligible for a District e-mail account. E-mail or network access accounts may be granted if directly sponsored by a District administrator.

C. **System Security Obligations**
   1. Users are responsible for the use of their individual access account(s) and should take all reasonable precautions to prevent others from being able to use their account(s), including coworkers, friends, or family. Under no conditions should a user provide his/her password to another person.
   2. Attempts to log on to the District's private network or any other network as a system administrator is prohibited.
   3. Any user identified as a security risk or having a history of violating this or any other Acceptable Use Policy may be denied access to the District's private network.
   4. Users will avoid the inadvertent spread of computer viruses.
   5. Users should immediately notify a teacher or system administrator of any possible security problem.
   6. Students will promptly disclose to their teacher or other appropriate school employee any message received that is inappropriate.
   7. Users may not connect unauthorized wireless devices to the District network. Wireless devices include, but are not limited to: wireless access points, wireless routers or any type of wireless gateway device.

D. **Filtering**
   1. As required by law and in recognition of the need to establish a safe and appropriate computing environment, the District will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet

E. **Unacceptable Uses**
   1. Users may not use the District's private network to access material that is profane or obscene (pornography of any kind), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
   2. Users may not post personal information on the Internet about themselves or other people. Personal contact information includes address, telephone, school address, work address, pictures or video bites, clips, etc.
   3. Users may not attempt to gain unauthorized access to any computer system. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing", "snooping", or "electronic discovery".
   4. Users may not deliberately disrupt or harm hardware or systems, interfere with computer or network performance, interfere with another's ability to use equipment and systems, or destroy data.
   5. Users may not use the District's private network to engage in illegal acts, such as threatening the safety of

another person, accessing or sharing unauthorized copyrighted music, movies, and other intellectual property, etc.

6. Users may not utilize peer-to-peer file-sharing applications or execute programs to facilitate the downloading or exchange of copyrighted or unauthorized music, movies, and other materials.
7. Users may not use the District's private network to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others.
8. Users may not post information that could endanger an individual, cause personal damage or a danger of service disruption.
9. Users may not knowingly or recklessly post false or defamatory information about a person or organization.
10. Users may not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
11. Users may not indirectly or directly make connections that create "backdoors" to the District, other organizations, community groups, etc. that allow unauthorized access to the District's network.
12. Users may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language.
13. Users may not engage in personal attacks, including prejudicial or discriminatory attacks. Users may not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
14. Users may not re-post a message that was sent to them privately without permission of the person who sent them the message.
15. Users may not forward or post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people. Users also must refrain from abusing email distribution lists. Acts of abuse include, but are not limited to: forwarding non-school/work related emails, advertising and solicitation.
16. Users may not install software of any kind on district machines. Authorized software will be installed by authorized personnel only. Users will not install or reproduce unauthorized or unlicensed software on District resources.
17. Users may not plagiarize works that they find on the Internet or other resources.
18. Users may not use technology resources and Internet for private business activities or unreasonable personal use.
19. Users may not use the District's private network for political lobbying.
20. Students will not download files unless approved by their teacher.
21. Users may not use any type of internet proxy service or proxy server to bypass district filters.
22. Users may not alter machine configurations or attempt to perform diagnostics or repairs on district machines. Diagnostics and repairs must be performed by authorized personnel only.

F. **Due Process**
1. The School District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the District's private network.
2. In the event there is an allegation that a student has violated the District Acceptable Use Policy, disciplinary actions may be taken.
3. Employee violations of the District Acceptable Use Policy will be handled in accordance with law, School Board Policy or collective bargaining agreement(s), as applicable.

G. **Administration**
1. Computer Aided Instruction has the responsibility and authority for the development, publication, implementation and ongoing administration and enforcement of the processes and techniques required to protect the Hobbs Municipal School District's technology systems and services from unauthorized access, loss or misuse.
2. School principals have the responsibility to establish a plan to ensure adequate supervision of students. They are also responsible for interpreting and enforcing this policy at the local level.
3. Local management has the responsibility to enforce and interpret this policy.