CUSHING INDEPENDENT SCHOOL DISTRICT

Acceptable Use Policy (AUP)

For Technology Resources

EDUCATIONAL PURPOSE

Network resources, including computers, hardware, software, file servers, and internet access, are available to students and staff in the Cushing Independent School District. Our goal in providing this service to students and staff is to promote educational excellence in the Cushing schools by facilitating resource sharing, innovation, and communication.

ACCESS

Technology access consistent with sound educational practice will be made available to students, staff, and community members in the Cushing Independent School District. No user shall be denied access because of gender, race, religious affiliation, age, ability level, socioeconomic level, language differences, handicapping condition, or other exceptionalities.

To gain access to network resources and the internet, all students and staff must sign the District Internet User Agreement form. Students under the age of 18 must obtain parental permission by having their parent or legal guardian sign and return the District form. Students 18 and over may sign their own forms. The Cushing ISD network must not be used for commercial, political, or illegal purposes. The District can revoke access to network resources, including the internet, if users exhibit unacceptable use of hardware, software, facilities, or network resources.

With the approval of the Principal and/or Technology Director, users will be granted appropriate access to the Cushing ISD network. A password will be assigned to each user. User accounts shall not be considered confidential, and may be monitored in order to track educational use of the CISD network.

- **In compliance with the Children's internet Protection Act ("CIPA")**, the School District's internet access includes filtering and/or blocking software to restrict access to internet sites containing pornography, obscene depictions, or other materials considered harmful to minors. Content will be filtered for both minors and adults. However, no software is foolproof, and there is still a risk an internet user may be exposed to a site containing controversial materials. A user who accidentally connects to such a site must immediately disconnect from the site and notify a teacher or supervisor. If a student sees another user is accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

- **Student use of the internet should be monitored at all times by the teacher or supervising staff member.** In compliance with CIPA, the School District and its representatives monitor all on-line activities. Monitoring is aimed to protect students from accessing inappropriate matter. The School District reserves the right to monitor other users' (e.g., employees or visitors using school resources) online activities, and to access review, copy, store or delete any electronic communications or files and disclose them to others as deemed necessary.

- **It is the responsibility of all Cushing ISD staff to educate, supervise, and monitor appropriate usage of the computer network and access to the internet** in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Before using online resources, all students must be taught appropriate use of network and internet resources as well as appropriate online behavior. This includes dialogue about internet safety, disclosure of personal information, and interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

- If a student under the age of eighteen accesses the internet outside of school, the parent or legal guardian is responsible for supervising the student's use of the internet and is completely responsible for monitoring its use.

- Procedures for the disabling or otherwise modifying any technology protection measures for bona fide research or other lawful purpose shall be the responsibility of the Technology Director or designated representatives.

RESPONSIBILITIES

The following guidelines are established so that all users are aware of the responsibilities they are about to acquire. In general, this requires efficient, ethical, and legal use of network resources. If the District user violates any of these provisions, his or her usage will be terminated and future access could be denied. All users are required to acknowledge receipt and understanding of the policy and guidelines. The signatures at the end of this document are legally binding and indicate that the parties who signed have read the terms and conditions carefully and understand their significance.

The District is responsible for securing its network and computing systems in a reasonable and economically feasible degree against unauthorized access or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of the policy and guidelines will result in disciplinary action in the form of temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocation can result from disciplinary actions taken by District administrators. The users of the network are responsible for respecting and adhering to local, state, federal, and international law. Any attempt to break those laws through the use of the network may result in action against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

PROHIBITED ACTIVITIES

The use of network resources, including the internet, through the District must be in support of education and research and be consistent with the educational objectives of the District. Use of any other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited.

Prohibited activities include, but are not limited to, the following:

- Reproducing copyrighted material without explicit permission
- Sending or displaying offensive messages or pictures
- Use of the network for commercial purposes
- Use of the network for political lobbying
- Downloading games or other unapproved software
- Trespassing in another user’s folders, work or files
- Using others’ passwords
- Harassing, insulting, or attacking others
- Using obscene, lewd, vulgar, rude, inflammatory, threatening or disrespectful language
- Any use that disrupts the educational and administrative goals of the District
- Damaging computers, computer systems or computer networks
- Misuse of computers, computer systems, printers, hardware or computer networks
- Unauthorized downloading of materials, including audio or video files
- Accessing material that has been deemed inappropriate for school use
- Plagiarizing works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- Unauthorized access (hacking) of web sites and password-protected folders.
- Any other activity identified as unlawful by school or law enforcement authorities

Violations may result in a loss of access as well as other disciplinary or legal action.

USE OF E-MAIL, CHAT ROOMS, INSTANT MESSAGING & OTHER DIRECT COMMUNICATION

The District does not provide personal student e-mail and students are prohibited from using personal e-mail while at school. Students are prohibited from using instant messaging, text messaging, chat or other methods of direct electronic communication while at school. Any student or staff member observing violation of this internet safety rule by a student should report it immediately to an administrator or the technology director.

DISCLOSURE OF PERSONAL INFORMATION

Students shall not reveal on the internet personal information about themselves or about other persons. For example, students should not reveal their full names, home addresses, telephone numbers, school addresses, or parents' names on the internet, unless it is through the supervised use of secure online educational sites such as online college application forms or FAFSA. When using District resources, school staff should supervise students closely and prepare them beforehand through instruction so the students understand the dangers of revealing personal information about themselves or about other persons.

SECURITY

Security on any computer system is a high priority, especially when the system involves many users. If a user believes he or she can identify a security problem on the network, the user must notify a system operator. Do not demonstrate the problem to other users. Do not use another individual's account. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to network resources, including internet access, as provided by the District.

VANDALISM

Vandalism will result in cancellation of privileges and may result in other disciplinary or legal action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, or the deliberate damage of computers, printers, or any other component of the district network. This includes, but is not limited to, the uploading or downloading or creation of computer viruses.

CONSEQUENCES OF VIOLATION

The use of the network and the internet is a privilege, not a right, and inappropriate use will result in a cancellation of this privilege. The system operators—defined as the professional staff members who are supervising student access—and District employees are responsible for the operation of the network and will deem what is inappropriate use. Also, the system operators may deny access at any time as required or as they deem appropriate and without notice. A user who is identified as having violated CISD Acceptable Use guidelines will be subject to disciplinary action consistent with district policies and regulations and/or appropriate legal action may be taken.

LEVELS OF OFFENSE

1st Unacceptable Offense

1. User accounts will be deactivated regardless of the success or failure of the violation attempt.

2. Administrators will determine length of deactivation and/or assign AEP depending on the violation.

2nd Unacceptable Offense

1. User accounts will be deactivated regardless of the success or failure of the violation attempt.
2. Violator will not be allowed access to computers anywhere on CISD campuses for four weeks and/or will be assigned to AEP depending on the violation.
3. Permanent access may be denied to any user identified as a security risk or as having a history of problems with computer systems.

3rd Unacceptable Offense

1. After a 3rd violation a user is defined as a "Frequent Violator". User accounts for frequent violators will be terminated for the remainder of the school year. AEP may be assigned depending on the violation.
2. Permanent access may be denied to any user identified as a security risk or as having a history of problems with computer systems.
3. The Principal will use Board Policy to determine credit earned in technology classes.

DISCLAIMER AND LIMITATION OF LIABILITY

Access to network resources, including the internet, is provided on an "as is, as available" basis. The District, its Board, agents, and staff members make no representations or warranties, whether expressed or implied, of any kind with respect to the internet services to be provided by the District, or any information or software accessed or received by the applicant or contacts made by the applicant, and disclaims any implied warranties, including any implied warranties of merchantability or fitness for a particular purpose. The system administrators and the District do not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements or that the operation of the system will be uninterrupted or error-free or that defects in the system will be corrected.

The District will not be responsible to users or liable for any claims, losses, or damages suffered as a result of these terms and conditions or users' access to internet service providers (ISPs), including without limitation, any losses, claims, or damages arising from the District's negligence or the users' own errors or omissions. The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or costs incurred by users. The user agrees that this limitation is intended to and does release the District from any claims, damages, or losses that may occur out of the use of this system. Use of any information obtained via a user's connection to the internet via the District system is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through this service.

APPLICATION OF TERMS AND CONDITIONS

All terms and conditions as stated in this document are applicable to the applicant's use of network resources, including internet resources, through the District. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Texas and the United States of America.

The signatures on the agreement document are legally binding and indicate that the parties who signed have read the terms and conditions carefully and understand their significance. Please

read this document carefully before signing.

APPEAL

Decisions under this policy may be appealed to the Board in accordance with policies DGBA(LOCAL) for District employees and FNG(LOCAL) for students and parents.

CUSHING INDEPENDENT SCHOOL DISTRICT
Internet User Agreement

Please sign and return this form to the campus principal's office.

Student name _____ Graduation year _____
(Please print)

STUDENT:

I have read and understand the District's Acceptable Use Policy for Network Resources. I agree to follow the rules contained in this Policy. I understand that if I violate the rules, access to network resources, including internet resources, can be terminated and I may face other disciplinary measures. Depending on the seriousness of the violation, appropriate legal action may be taken.

_____ _____
Date Student signature

****

PARENT OR GUARDIAN: A parent or guardian must also read and sign this agreement.

As the parent or guardian of the above student, I have read the attached Acceptable Use Policy for Cushing ISD. I understand that this access is designed for educational purposes. I also recognize that it is impossible for the District to restrict access to all controversial materials, and I will not hold them responsible for controversial materials acquired on the internet or for the unauthorized use of the system to purchase products or services. I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set forth in the District Acceptable Use Policy. I will emphasize to my child the importance of following the rules for personal safety. Further, I accept full responsibility for supervision if and when my child's use of the internet is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

_____ _____ _____
Date: Parent/Guardian Name: (please print) Parent/Guardian Signature:

****

At various times throughout the school year, the District may display student photos in a group setting on the District's web site–for example, team pictures or athletic events. Students' full names are not published. If names are included, first name/last initial or first initial/last name may be used.