Dilley ISD
Acceptable Use
Policy

The Dilley ISD has made Internet access available to the staff and students of the District and believes the Internet offers a multitude of valuable resources and ways of enhancing the educational experience.

The Internet is an electronic highway connecting millions of computers all over the world to billions of individual subscribers who have access to electronic mail communication with one another. Further, the Internet provides users with information and news from research institutions, colleges and libraries, including discussion groups on a wide variety of topics. With access to computers and people all over the world, also comes the availability of material that may not be considered to have educational value in the context of the school environment. Although Dilley ISD uses filters to restrict access and protect its students and staff from harmful material, it is impossible to restrict all harmful materials. Ultimately, the responsibility to avoid harmful material rests with the user, who must adhere to the District's strict guidelines. These guidelines are provided so that users are aware of the responsibilities they acquire when accessing the District's network. In general, the responsibilities include efficient, ethical, and legal utilization of the District's network resources.

It is important that you read all Dilley ISD polices, and ask questions if you need help in understanding them. If you violate any of these provisions, your network access account may be terminated, and future access denied. Acceptance of this Acceptable Use Policy ("AUP") is construed at time of receipt.

Definition of Harmful Material

Material that is harmful to students and minors means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to students and minors, appeals to a prurient interest in nudity, sex or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for students and minor, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals.
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to students and minors. 47 U.S.C. 254(h)(7)(G); 20 U.S.C. 6777(e)(6).

District Level

The District's system shall only be used for administrative and educational purposes that are consistent with the District's mission and goals. Commercial, income-generating, or "for profit" use of the District's system is strictly prohibited. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost to the District;
2. Does not unduly burden or increase the security risk of the District's computer network or resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Filtering

Electronic mail transmissions and other use of the electronic communications shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for educational or administrative purposes. Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

System Access

Dilley ISD controls students' access to inappropriate materials, as well as materials that are harmful to minors. DISD also makes every effort to ensure student safety and security when using District electronic communications including a) preventing unauthorized access, hacking and other unlawful activities, b) restricting unauthorized disclosure, use, and dissemination of personally identifiable information regarding students, and c) educating students about digital citizenship such as cyber bullying awareness and response, as well as appropriate online behavior.

System Access

Access to the District's technology resources, including electronic communication devices and computers, is a **privilege**—not a right. Access may be made available to students and employees primarily for instructional purposes, and in accordance with this AUP, District policy, and state and federal guidelines. Access shall be given to all employees as a privilege via a standard user account. This standard user account allows for internet access and access to District resources. If any program must be installed to further educational or instructional purposes, the installation must be completed through the appropriate technology personnel. If additional software is necessary for classroom instruction, staff shall contact the technology department at least one (1) day prior to the day the software is necessary for instruction, in order for the software to be installed and prepared by the day of instruction.

User Responsibility

The following standards apply to **all** users of the District's communications systems and network resources:

1. Revealing your personal information or the personal information of others is prohibited.
2. Be polite. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
3. Users shall not use the computer to harass others with language, images, or threats.
4. Users shall not deliberately access or create any harmful material, as described above.
5. The individual in whose name a system account is registered and/or used is responsible for use of the system account at all times, and shall not allow others to use their login information (except for authorized staff members).
6. Users may not install any program or software unless approved through the technology department.
7. Users shall not intentionally damage the District's account system or network resources through physical abuse or software manipulation.

Failure to comply with any of the above standards may result in disciplinary action, up to and including suspension, expulsion, or termination.

Inappropriate uses

- Using technology resources for any illegal purpose or in violation of District policy.
- Damaging electronic communication systems or electronic equipment including: a) knowingly or intentionally introducing a virus to a device or network, or not taking proper security steps to prevent a device or network from becoming vulnerable; b) disfiguring or altering equipment, or displaying lack of reasonable care in its use.
- Disabling or attempting to disable any Internet filtering device. Requests to disable a filtering device should be made to the District's technology coordinator.
- Accessing sites not authorized under the District's filtering policies.
- Encrypting communications to avoid security review.
- Using any account or login credentials other than your own.
- Sharing your account or login credentials with anyone else.
- Pretending to be someone else when posting, transmitting, or receiving messages.
- Attempting to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.
- Using resources to engage in conduct that harasses or bullies others.
- Posting, transmitting, or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Using inappropriate language such as swear words, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- Posting or transmitting pictures of students without obtaining prior permission from all individuals depicted or from parents or guardians of depicted students who are under the age of 18.
- Violating others' intellectual property rights, including downloading or using copyrighted information without permission from the copyright holder.
- Use of unlicensed software, or altering District installed software.
- Wasting school resources through improper use of the District's technology resources, including creating and distributing chain letters, sending spam, or setting up equipment so that it can act as an "open relay" for third-party spammers, or providing products or services for pay, i.e., outside employment.
- Sending unauthorized broadcasts to official or private distribution lists, regardless of content or recipients.
- Gaining unauthorized access to restricted information or resources.

If you are a student:

- Posting or transmitting personal information about yourself or others, such as addresses and phone numbers.
- Responding to requests for personally identifying information or contact from unknown individuals.
- Making appointments to meet in person people met online. If a request for such a meeting is received, it should be reported to a teacher or administrator immediately.

Report Violations

The District plays an active role in monitoring all activities that take place on the Dilley ISD Network. Daily monitoring of internet usage is taking place, and violations shall be reported to appropriate campus personnel within 48 hours of its detection. All District personnel shall report any known violation of this Acceptable Use Policy. Students must report known violations to their supervising teacher, or a technology department employee. Employees and students must report requests for personally identifying information, or similar conduct from unknown individuals, as well as communication that is or related to:

- Abusive
- Obscene
- Online Gambling
- Sexually-Oriented Material
- Threatening/Harassing
- Damaging to another person's reputation
- Promoting Violence
- Illegal
- Harmful Material

Educational Materials

Educational materials regarding the proper use of District technology resources shall be provided for employees and students, with an emphasis on safe and ethical use of technology and awareness of the District's AUP. This information helps to promote an environment of safety pertaining to electronic communication, including: internet use, technical interaction, appropriate online behavior, awareness of cyber-bullying, and responding to cyber-bullying. Each campus shall provide training on appropriate online behavior, and cyberbullying awareness and response.

Termination/Revocation of System User Account

The District may suspend or revoke user access to the District's system based on violation(s) of this AUP, District policy, and/or administrative regulations regarding acceptable use. A student or employee who knowingly introduces prohibited materials into the District's electronic environment shall be subject to suspension and/or other disciplinary actions in accordance with District policies and this AUP.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, with respect to any services provided by the system(s) and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communication system(s).

Disclaimer of Liability

The District shall not be liable for the users' inappropriate use of the District's electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet. The Superintendent or designee will oversee the District's electronic communication system(s). Oversight of the posting of official district, campus, or division/department materials on the District's electronic communication system(s) will be the responsibility of the superintendent, principal, or division/department supervisor or designee. The District's system(s) will be used only for administrative and instructional purposes consistent with the District's mission and goals.

Copyright

Copyrighted software or data may not be placed on any system connected to the District's system(s) without permission from the holder of the copyright. Only the owner(s) or individuals the owner(s) specifically authorized may upload copyrighted material to the system(s).

I understand that my use/my student(s)' use of the District's technology resources is not private and that the District will monitor my/my student(s)' activity. I have read these acceptable use guidelines and agree to abide by the provisions. I hereby release the District, its operators, and any of its affiliated institutions from any and all claims and damages of any nature arising from my use of or inability to use these resources, including without limitation, the type of damages identified in the District's policies and administrative regulations.

Signature ____ Date _______________________________________

Parent/Guardian Signature _______________________________________ Date_______________________________________