TWIN HILLS SCHOOLS
ACCEPTABLE USE AND INTERNET SAFETY POLICY

The Board of Education of Twin Hills Public Schools recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, Twin Hills Public Schools will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

The Board directs the Superintendent to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

Acceptable Use and Internet Safety

These procedures are written to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behaviors online are no different than face-to-face interactions.

I. Network

The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Connection of staff personal computers to the district network after checking with the technology director to confirm that the computer is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by district students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;

- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the technology director;
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
- Unauthorized access to other district computers, networks and information systems;
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

II. Internet Safety

Personal Information and Inappropriate Content

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring

To the extent practical, technology protection measures (Internet content filters) shall be used to block or filter user access over the district's computer network to inappropriate information. Specifically, as required by the Children's Internet Protection Act (CIPA), blocking or filtering shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Other objectionable material could be blocked or filtered. The determination of what constitutes "Other objectionable" material will be determined as necessary by the district.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering the district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;

- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

III. Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

IV. Network Security and Privacy

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communication;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen, or log off, if leaving the computer.

Student data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

No Expectation of Privacy

The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Oklahoma.

V. Education, Supervision and Monitoring

It shall be the responsibility of the Twin Hills Public Schools staff to supervise and monitor appropriate usage of the online computer network and access to the Internet.

It shall be the responsibility of all members of the Twin Hills Public Schools staff to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response, as required by the Children's Internet Protection Act.

VI. Disciplinary Action

The user's use of the District's computer network and the Internet is a privilege, not a right. All users of the District's electronic resources are required to comply with this Acceptable Use and Internet Safety Policy. A user who violates the Policy, shall be at a minimum, have his or her access to the computer network and Internet terminated, which the District may refuse to reinstate for the remainder of the student's enrollment in the 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 or Internet, including any user whose access had been denied or terminated. The District may also take other disciplinary action in such circumstances. In some instances, inappropriate computer and Internet use violates state and/or federal laws and may result in criminal prosecution or juvenile court action.

STUDENT’S AGREEMENT

Every student, regardless of age, must read and sign below:

I have read, understand, and agree to abide by the terms of the foregoing Acceptable Use and Internet Safety Policy. Should I commit any violation or in any way misuse my access to the District’s computer network and the Internet, I understand and agree that my access privilege may be revoked and School disciplinary action may be taken against me.

______________________________ ______________________________
Student Name (Please Print) Home Phone

______________________________ ______________________________
Student Signature Date

PARENT’S OR GAURDIAN’S AGREEMENT

____
Student’s Name (Please Print)

To be read and signed by parent or guardian of student:

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 District’s Acceptable Use and Internet Safety Policy for the student’s access to the District’s computer network and the Internet. I understand that access is being provided to the students for educational purposes only. I understand that it is impossible for the District to restrict access to all offensive and controversial materials and understand my child’s or ward’s responsibility for abiding by the Policy. I am therefore signing this Policy and agree to indemnify and hold harmless the School, the School District, and the Internet provider against all claims, damages, losses, and costs, of whatever kind that may result from my child’s or ward’s use of his or her access to such networks or his or her violation of the foregoing Policy. Further, I hereby give permission for my child or ward to use the District’s computer network and the Internet.

______________________________ ______________________________
Parent/Guardian Name (Please Print) Home Phone

______________________________ ______________________________
Parent/Guardian Signature Date