Todd County Schools Acceptable Use Policy
2014-2015 School Year

The Todd County Board of Education believes the use of technology enhances the District's educational environment and allows access to resources that maximize teaching and learning. As explained by Board Policy 08.2323, the Board supports the privilege of students and staff to have reasonable access to various electronic information. Electronic access including Internet, e-mail, the District's internal network, and to any other technology resource via the internal network. Access to the network is given to staff and students who agree to act in a responsible manner. Access to the network and resources is a privilege not a right. Access is granted to District owned technology only, in accordance with Kentucky Department of Education (KDE) guidelines, and District policy, staff or students are not permitted access to the state's network using personally owned technology. Access can be revoked for improper usage, and legal and/or disciplinary actions, if warranted, may be taken.

Procedures and Guidelines for Gaining Access to District Resources

The Todd County Schools Acceptable Use Policy specifies acceptable use, rules of on-line behavior, and the penalties for violations. The signed user agreement shall be kept on file and is a legally binding document. All District classrooms are wired and permit access to the District network. Both staff and students shall have user/e-mail accounts on the network. Users are responsible for all activities associated with their account and for the security of their password. All users, and/or parent or legal guardian, shall sign the District Acceptable Use Policy as a pre-requisite to being allowed access to their user account. In the event the user agreement is withdrawn, access shall be terminated.

Internet Safety Policy

The Children's Internet Protection Act (CIPA) enacted in 2000 requires web content filtration and monitoring the online activities of minors. Filtration is defined as: blocking inappropriate content. The District utilizes filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. These measures filter online access both in district and on the District owned devices that travel home with students. Monitoring is defined as requiring supervision, not technical measures. Instructional staff is instructed to and shall actively supervise their students when they are using any form of technology.

The safety of our staff and students is of the upmost importance to the District. While our intent is to insure their safety, users may find ways to access objectionable material. Although the District takes measures to prevent this, all parties need to be aware that this is possible. The use of anonymous proxies, or other measures, to get around the content filter is strictly prohibited and will be considered a violation of this policy.

Students in grades K-12 will be provided age appropriate instruction about Digital Fluency, including but not limited to Internet safety, appropriate online behavior, and cyber-bullying. 082323.AP.1

Privacy Notice

No employee or student has a right to expect privacy while using District networks or hardware. The CIO or designee has the right to access any and all information in any user directory, on the current user screen or in electronic mail. Electronic mail is not private. Users are advised not to place confidential or objectionable documents in their user directory. The CIO/designee may periodically examine Internet activity to detect access to inappropriate or unauthorized information or websites. The CIO shall also periodically monitor electronic MAIL to ensure that staff or students are using KETS approved mail systems. The CIO/designee may also monitor drives and external storage devices (flash and jump drives, CDs, etc) connected to and used on district resources/computers. The CIO or designee may close an account at any time. The administration of each school in the District may also deny, revoke, or suspend specific use accounts at their facility. Their decision shall be final.

Vandalism

Vandalism shall result in a loss of privileges. Vandalism is defined as any attempt to access, harm or destroy data, operating systems or applications of another user, the school's network or any of the agencies of other networks that are connected to KETS Internet structure. This includes the uploading or creation of computer viruses and or malware.

Legal Issues

The terms and conditions of this policy shall be interpreted, construed and enforced in accordance with the laws of the state of Kentucky:

- Criminal Damage to Property Law, Class D Felony KRS 512.020
- Unlawful Access to a Computer, Class C Felony KRS 434.840-434.860
- Open Records Law, KRS 61.870-61.884 and KRS 171.410 –171.720
- KRS 156.675; 701 KAR 5: 120

Copyrighted Materials

The use of copyrighted material for educational purposes, by school personnel, shall be within the generally accepted uses delineated by applicable law. All employees shall use electronic materials only in accordance with the license agreement under which the electronic materials were purchased or otherwise procured. Electronic materials are defined as software, photos, music, videos, websites, electronic textbooks or any other copyrighted material distributed in electronic form. Any duplication of copyrighted electronic materials, except for backup and archival purposes, is a violation of the law, unless the license agreement explicitly grants duplication rights. The archival copy is not to be used on a second computer at the same time the original is in use. In addition, illegal copies of copyrighted software shall not be used on District equipment. The Superintendent/designee shall sign all District software license agreements. The CIO shall have on file a copy of all executed software licenses or original documentation of software purchased by the District. Employees shall have on file a copy of all executed software licenses, the original disk or the original documentation of software purchased for their individual workstations. Employees shall not install any software on individual workstations without permission from the CIO.

Network, E-mail and Internet Regulations

The use of network and/or Internet accounts must be in support of education and research and be consistent with the educational objectives of the District. Staff members shall supervise student use of network resources (including, but not limited to, internet and email). Parents/Legal guardians should accept responsibility for guiding their child in the appropriate use of Internet/e-mail.

Only KETS approved e-mail may be utilized on the District network. All District users shall access District resources by logging on and logging off each time they use a computer. The use of this account to send non-educational/non-work related mass emails is prohibited. Mass email is defined as sending to all students or all staff. Please be responsible when sending emails, do not attach large files (i.e., photos, music, videos, etc.).

Publishing student pictures and work on websites promotes learning, collaboration and provides an opportunity to share the achievements of students. Images and products of K-12 students may be included on the website without identifying captions or names. Parents/guardians must indicate their written consent to publish their child's photo or school work on any school related website before the item is published to the web. Please note that under no circumstances will K-12 student photos or work be identified with first and last name on website, including the district, school, or teacher website.

Unacceptable use may include:

- Uses that cause harm to others or damage to their property. For example, do not engage in defamation (harming another's reputation by lies); do not employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; do not upload a virus, trojan horse, time bomb, or other harmful form of programming or vandalism; do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.

- Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, do not disclose or share your password with others; do not impersonate another user.
- Uses that are commercial transactions. Students may not use the school network to sell or buy anything over the Internet.
- Illegal activities, including copyright or contract violations shall not be permitted on the Internet.
- Email/Internet shall not be used for commercial, political, illegal, financial, or religious purposes.
- Threatening, profane, harassing, bullying or abusive language shall be forbidden.
- Use of the network for any illegal activities is prohibited. Illegal activities include (a) tampering with computer hardware or software, (b) vandalism or destruction of equipment, (c) using another user's password, or gaining unauthorized access to computers or computer systems, or attempting to gain such unauthorized access and (d) deletion of computer files. Such activity is considered a crime under state and federal law.
- Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
- No user is permitted to knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.
- Invading the privacy of another user, using another's account, posting personal messages without the author's consent, and sending or posting anonymous messages is forbidden.
- Accessing pornographic or obscene materials, or using or sending profanity in messages is forbidden.
- The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.
- Sending mass emails to all students or staff; forwarding of junk emails and/or chain letters
- Harassing, bullying, insulting or threatening others on the network, internet or via email

Safety Concerns:

- Parents and Users. Despite every effort for supervision and filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
- Personal Safety. In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.
- Confidentiality of Student Information. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian.

Use of Web Tools-Web 2.0 tools

Online communication and collaboration is critical to our students' learning of 21st Century Skills and tools such as blogs, wikis, social networking and hosted services offer an authentic, real-world vehicle for student expression. As educators, our primary responsibility to students is their safety. Hence, expectations for classroom use of Web 2.0 tools must follow all established Internet safety guidelines. Many of these tools gather identifying information from children under age 13 and they must comply with the federally mandated Children's Online Privacy Protection Act (COPPA). Which means the tool must gain parental permission for the end user (student) to use the tool. It is up to the teacher to read through the Terms of Service for each tool to understand how this permission must be gained and granted. The district Acceptable Use Policy (AUP) does not cover the use of these tools without additional parent permission. The teachers must (1) educate themselves on any age restrictions (2) send out a parent permission form that outlines how you will be using this tool and get parent signatures.

Terms and Conditions:

- The use of web 2.0 tools is considered an extension of your classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all web tools. This includes but is not limited to; profanity, racist, sexist, harassing, threatening, bullying or discriminatory remarks.
- Students using Web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts.
- NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.

- Never link to web sites without reading the entire article to make sure it is appropriate for a school setting.
- Students who do not abide by these terms and conditions shall lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Violations of the Acceptable Use Policy

Violations of the Acceptable Use Policy may result in the immediate loss of network services. Violations may result in disciplinary action by the school and/or legal action by the Board. The CIO/designee may suspend, deny or revoke specific user accounts at any time. Staff members and students whose accounts have been suspended, denied or revoked do have the following rights:

- To request, in writing, a written statement justifying the action
- To follow the District's grievance procedure.

Users and/or parent or legal guardian's signature acknowledges that you accept and agree that you/your child's rights to use the electronic resources provided by the District and/or the Kentucky Department of Education (KDE) are subject to the terms and conditions set forth in District policy/procedure. Please also be advised that data stored in relation to such services is managed by the District pursuant to policy 08.2323 and accompanying procedures. Users and/or parent or legal guardian also understand that the email address provided to your child can also be used to access other electronic services or technologies that may or may not be sponsored by the District, which provide features such as online storage, online communications and collaborations, and instant messaging. Use of those services is subject to either standard consumer terms of use or a standard consent model. Data stored in those systems, where applicable, may be managed pursuant to the agreement between KDE and designated service providers or between the end user and the service provider. Before you/your child can use online services, you/he/she must accept the service agreement and, in certain cases, obtain parental/guardian consent.