Todd County Schools Acceptable Use Policy
21-22 ~~2020-2021~~~~2018-2019~~ 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 In the event the user agreement is withdrawn, access shall be terminated.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 are 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 cyberbullying. 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.

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

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.**

Formatted: Font: Bold

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.).

Formatted: Font: Bold

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.**

Technology-based materials, activities and communication tools shall be appropriate for and within the range of the knowledge, understanding, age and maturity of students with whom they are used. District employees and activity sponsors may set up blogs and other social networking accounts using District resources and following District guidelines as explained by Board Policy 08.2323 to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction. Networking, communication and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

Incidental personal uses of Internet and E-mail resources are permissible, but not encouraged. Excessive personal use shall lead to loss of the resource privileges and may result in disciplinary action pursuant to KRS 161.790 and all other applicable law~~18.A~~ up to and including dismissal. Staff members are responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or E-mail resources must adhere to the following limitations:

- It must not cause any additional expense to the Commonwealth or the staff members agency
- It must be infrequent and brief
- It must not have any negative impact on the staff members overall productivity
- It must not interfere with the normal operation of the staff members agency or work unit
- It must not compromise the staff members agency or the Commonwealth in any way
- It must be ethical and responsible.

Unacceptable use may include but are not limited to:

- 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 work, 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 personal business, commercial, political, illegal, financial, or religious purposes.
- Sending or forwarding chain letters or other pyramid schemes of any type.
- Sending or forwarding unsolicited commercial E-mail (spam) including jokes.
- Soliciting money for religious or political causes, advocating religious or political opinions and endorsing political candidates.
- 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) knowledgeable 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.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or E-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of E-mail.
- 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
- Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency or size of messages. This includes statements, language, images, E-mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- Making fraudulent offers of products, items, or services originating from any Commonwealth account.
- Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy as defined in the Kentucky Open Records Act, KRS 61.870 – 61.884.
- Online investing, stock trading and auction services such as eBay unless the activity is for Commonwealth business.
- Developing or maintaining a personal web page on or from a Commonwealth device.
- Use of peer-to-peer (referred to as P2P) networks such as Napster, Kazaa, Gnutella, Grokster, Limewire and similar services.
- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to: Internet games, online gaming, unnecessary Listserve subscriptions, E-mail attachments, chat rooms and messaging services.

- Staff shall be aware that their conduct or information they publish could reflect on the reputation of the Commonwealth. Therefore, professionalism in all communications is of the utmost importance.
- Staff members who choose to use E-mail to transmit sensitive or confidential information should encrypt such communications using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services.
- Staff shall represent themselves, their agency or any other state agency accurately and honestly through electronic information or service content.

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.

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.