Access to Electronic Media

The Board supports reasonable access to various information formats for students, staff and the community and believes it is incumbent upon users to utilize this privilege in an appropriate and responsible manner as required by this policy and related procedures, which apply to all parties who use District technology.

SAFETY PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for access to electronic media. Guidelines shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail and other District technological resources), and issues of privacy versus administrative review of electronic files and communications. In addition, guidelines shall prohibit utilization of networks for prohibited or illegal activities, the intentional spreading of embedded messages, or the use of other programs with the potential of damaging or destroying programs or data.

Students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber-bullying awareness and response.

Internet safety measures, which shall apply to all District-owned devices with Internet access or personal devices that are permitted to access the District's network, shall be implemented that effectively address the following:

- Controlling access by minors to inappropriate matter on the Internet and World Wide Web;
- Safety and security of minors when they are using electronic mail, chat rooms, and other forms of direct electronic communications;
- Preventing unauthorized access, including "hacking' and other unlawful activities by minors online;
- Unauthorized disclosure, use and dissemination of personal information regarding minors; and
- Restricting minors' access to materials harmful to them.

A technology protection measure may be disabled by the Board's designee during use by an adult to enable access for bona fide research or other lawful purpose.

The District shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate, its initial Internet safety measures.

Specific expectations for appropriate Internet use shall be reflected in the District's code of acceptable behavior and discipline including appropriate orientation for staff and students.

PERMISSION/AGREEMENT FORMS

A written parental request shall be required prior to the student being granted access to electronic media involving District technological resources.

Access to Electronic Media

PERMISSION/AGREEMENT FORMS (CONTINUED)

A written parental request shall be required prior to the student being granted access to electronic media involving District technological resources.

The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations, must be signed by the parent or legal guardian and also by the student. This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian must provide the Superintendent with a written request.

A written request/agreement and one (1) day of professional development training/awareness addressing the use of Internet and or e-mail shall be required prior to the staff members being granted independent access to electronic media involving District technological resources.

The required request/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations, must be signed by the staff members. This document shall be kept on file as a legal, binding document.

EMPLOYEE USE

Employees shall not use a code, access a file, or retrieve any stored communication unless they have been given authorization to do so. (Authorization is not required each time the electronic media is accessed in performance of one's duties.) Each employee is responsible for the security of his/her own password.

Employees are encouraged to use electronic mail and other District technology resources to promote student learning and communication with the home and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

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 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.

In order for District employees and activity sponsors to utilize a social networking site for instructional, administrative or other work-related communication purposes, they shall comply with the following:

1. They shall request prior permission from the Superintendent/designee.
2. If permission is granted, staff members will set up the site following any District guidelines developed by the Superintendent's designee.

Access to Electronic Media

EMPLOYEE USE (CONTINUED)

3. Guidelines may specify whether access to the site must be given to school/District technology staff.
4. If written parental consent is not otherwise granted through AUP forms provided by the District, staff shall notify parents of the site and obtain written permission for students to become "friends" prior to the students being granted access. This permission shall be kept on file at the school as determined by the Principal.
5. Once the site has been created, the sponsoring staff member is responsible for the following:
   a. Monitoring and managing the site to promote safe and acceptable use; and
   b. Observing confidentiality restrictions concerning release of student information under state and federal law.

Staff members are discouraged from creating personal social networking sites to which they invite students to be friends. Employees taking such action do so at their own risk.

All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

PARENTAL PORTALS

Access to the Parent Portal is a privilege, not a right. Users of the portal shall follow the District's Acceptable Use Policy (Access to Electronic Media) and accompanying procedures. In addition, any guidelines set forth by KDE concerning the use or misuse of the data system shall be followed.

Parents/guardians are responsible for their use of the Parent Portal. The District makes no guarantee that the Parent Portal will be error-free or without defect. The District is not responsible or liable for any damage that a user may suffer as a consequence of using the Parent Portal or information contained in the Parent Portal.

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which computer equipment, software and information access systems will be available to the community.

Upon request to the Principal/designee, community members may have access to the Internet and other electronic information sources and programs available through the District's technology system, provided they attend any required training and abide by the rules of usage established by the Superintendent/designee.

Access to Electronic Media

DISREGARD OF RULES

Individuals who refuse to sign required acceptable use documents or who violate District rules governing the use of District technology shall be subject to loss or restriction of the privilege of using equipment, software, information access systems or other computing and telecommunications technologies.

Employees and students shall be subject to disciplinary action, up to and including termination (employees) and expulsion (students) for violating this policy and acceptable use rules and regulations established by the school or District.

RESPONSIBILITY FOR DAMAGES

Individuals shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care. Students or staff members who deface a District web site or otherwise make unauthorized changes to a web site shall be subject to disciplinary action, up to and including expulsion and termination, as appropriate.

RESPONDING TO CONCERNS

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

AUDIT OF USE

Users with network access shall not utilize District resources to establish electronic mail accounts through third party providers or any other nonstandard electronic mail system.

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters Internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
2. Maintaining and securing a usage log; and
3. Monitoring online activities of minors.

ACCESS PRIVILEGES TO ELECTRONIC MATERIALS

Access to electronic information resources can range from read-only access to instructional software to full search capability of the Internet. For these reasons, schools maintain the right to limit access to software and/or documents found either on TCPSNet or the Internet via technical or human barriers.

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least ten (10) years after the last day of service in a particular funding year.

Access to Electronic Media

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 005:120
16 KAR 1:020 KAR 001:020 (Code of Ethics (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 47 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516
15-ORD-190

RELATED POLICIES:

03.13214/03.23214; 03.1325/03.2325; 03.17/03.27
08.1353, 08.2322
09.14, 09.421, 09.422, 09.425, 09.426; 09.4261
10.5

Adopted/Amended: 8/11/2015
Order #: 25

Access to Electronic Media

The Taylor County School District is pleased to offer its students, staff, and members of the community access to the District's computer network for Internet and Email use. This access includes access to the Internet, email (for grades 3-12), the District's internal network, and any other technology resources including computers, tablets accessed via that internal network (from this point on, all of these resources will be referred to simply as "The Network"). To gain access to the Network, all students and employees must complete, sign, and return an Access to Electronic Media/User Agreement Form (09.2323 AP.1) to the Principal/designee prior to access/use.

While our intent is to make Internet and Email access available to further educational goals and objectives, it is possible that students might find ways to access other materials as well. Although the District does implement filters to decrease the risk, families should be warned that some material accessible via the Internet may contain items and information that are illegal, defamatory, inaccurate, or sexually explicit, or otherwise potentially offensive to some people.

Except in cases involving students who are at least eighteen (18) years of age and have no legal guardian, parents/guardians may request that the school/District:

- Provide access so that the parent may examine the contents of their child(ren)'s email files and Internet history;
- Terminate their child(ren)'s individual email account and/or Internet access; and
- Provide alternative activities for their child(ren) that do not require Internet access.

Parents wanting to challenge information accessed via the District's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

General Standards for Users

Users are required to comply with District standards and to honor the access/usage agreements they have signed.

The network is provided for users to conduct research and to communicate with others. Within reason, freedom of speech and access to information will be honored. During school hours, teachers of younger children will guide their students to appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio, and other media that may carry/broadcast information.

Access to the Network is given to users who agree to act in a responsible manner. Access is a privilege—not a right. Access can be revoked for improper usage, and legal or disciplinary actions, if warranted, may be taken. The District is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network independently of the District's filtering solution (proxy).

Network storage areas are treated like school lockers. Administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Files stored on District computers or servers are not private. Users should not expect that anything they do on the Network will be private.

Rules and Regulations [ALL]

The rules listed below apply to all forms of system usage including but not limited to, Internet access, email, and social networking. Violation of any of the rules below or any part of the District Acceptable Use Policy may result in disciplinary action.

Access to Electronic Media

RULES AND REGULATIONS (CONTINUED)

- The use of your account must be in support of education/research and be consistent with the educational objectives of the District.
- You shall not violate State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination or personal information.
- You shall not give your password to anyone nor let any individual access the Internet via your account.
- You shall not log on with or use any other person's password or account.
- You shall not post or exchange personally identifiable information (such as your full name, date of birth, address, phone number, financial information, Social Security Number, etc.) on the Network without permission from District personnel.
- You shall not transmit or access obscene, abusive or sexually explicit language.
- You shall not create or share computer viruses.
- You shall not trespass into another person's folder, work or files.
- You shall not copy material from the Internet and represent it as your own (plagiarism).
- You shall not use the Network for commercial purposes, excessive personal use, financial gain, or illegal activity.
- You shall not monopolize the resources of the District Network by such things as running large programs and applications over the network during the day, sending massive amounts of email to other users, downloading high bandwidth files (such as videos or music files) that are not related to educational objectives, or using system resources for games.
- You shall not access, copy or transmit another user's messages without permission. Only send electronic messages using your own name and/or account.
- You shall not break or attempt to break into secure areas of this Network or other computer networks.
- You shall not interfere with, sabotage, or vandalize the computer hardware or software of others, including the District.
- You may not access the District's computers remotely unless specific access has been granted by the District.
- You shall not alter the Network system files for any reason.
- You shall not get software from or put software onto the Network without first obtaining written pre-approval from school personnel.
- You shall not get from or put onto the Network anything that may be considered threatening, lewd, vulgar, or otherwise sexually explicit.
- You shall not violate any copyright or software license.
- You shall not circumvent security measures of the computer or the Network. This includes using a "proxy redirect" website or program to access web pages that have been blocked by the Taylor County technology department.

Access to Electronic Media

RULES AND REGULATIONS (CONTINUED)

- You shall not connect to wireless networks other than the District supplied wireless network.
- You shall not promote any illegal conduct or the use of drugs, alcohol, or tobacco.
- You shall not use the Network to harass any person sexually nor shall you harass or discriminate against any person on the basis of race, color, national origin, religion, gender, age, and disability.
- You shall not send or display offensive messages or pictures, including those that involve: profanity, obscenity or harassing or intimidating communications.
- You shall not post photographs without permission.
- You shall not use technology resources to bully, threaten or attack a staff member or student or to access and/or set up unauthorized blogs and online journals.
- You shall not damage school computers or other technology equipment.
- As a user of the Network, students should notify an administrator or teacher of any violations of this contract taking place by other users or outside parties. This may be done anonymously.
- A student who does not have a signed AUP on file may **not** share access to the network with another student (e.g. "looking over the shoulder" of another student who is accessing the Internet or working together on an Internet project with a student who has permission).

ADDITIONAL RULES AND REGULATIONS MAY BE FOUND IN DISTRICT HANDBOOKS AND/OR OTHER DOCUMENTS. VIOLATIONS OF THESE RULES AND REGULATIONS MAY RESULT IN LOSS OF ACCESS/USAGE AS WELL AS OTHER DISCIPLINARY OR LEGAL ACTION.

EMPLOYEES

- Employees are responsible for the security of their passwords.
- Employees are to ensure that their workstation or device is "locked" when it is unattended. Failure of employees to secure their workstation will be reported to the employee's supervisor.
- Internet safety and digital citizenship for students will take place at the beginning of each year and upon enrollment of new students.
- Teachers and staff will actively monitor student technology use.
- Teachers and staff will monitor the safety and protection of district devices, reporting any damaged or missing devices immediately to building or district administrators.
- Employees who elect to use third-party resources for notifications (i.e. Remind) are responsible for the members in the group(s) and the content of the conversations. Such sites must be closely monitored by the employee to ensure conversations are appropriate. Private messaging between members of the group and students is strictly prohibited. Access to members and conversations in such apps are subject to review by school and District personnel.

Access to Electronic Media

EMPLOYEES (CONTINUED)

- Employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory, or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to the Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up tot and including termination.

COMMUNITY USE

- Community members may request access to the Internet and other electronic information sources and programs available through the District's technology system by submitting an agreement form to the Principal/designee of the school through which access is sought.
- Permission will be granted only after the individual completes training required by the Principal/designee appropriate for the access requested.

SOCIAL NETWORKING

- Social networking sites, may only be accessed if the following three criteria are met: 1) Access to such sites is for educational use and supports the educational objectives of the Taylor County School District. 2) You are directly supervised by a teacher or other staff member who is aware of and approves of your attempt to access such a site. 3) Such sites are not blocked by the district technology department.
- Students shall not reveal their name or Personally Identifiable Information to, or establish relationships on the Internet unless a parent or teacher has coordinated the communication.
- Students who utilize social networking for educational purposes shall be aware of and familiar with privacy options on the social networking site, and shall set those options to limit access to personal information to "friends" only.
- Students and parents shall be aware, however, that privacy options alone can never fully protect personal information. If a student shares personal information with "friends," those friends may share that information with others. With this in mind, students shall carefully consider what information is posted online.
- Photos posted on social networking sites that you are using for educational purposes shall NOT contain other students. Permission, either spoken or in writing, should be granted from any adults before posting their pictures.
- Teachers and other adult staff have been advised NOT to "friend" students on social networking sites using the same account used for personal social networking. Students are given the same advice. Remember that teachers are ethically and legally bound to report any activity in which a student may be breaking the law or may be in danger of hurting him/herself or others.
- As mentioned in the "RULES AND REGULATIONS" section, you shall not utilize social networking sites to harass or bully others.

Access to Electronic Media

PERSONALLY-OWNED DEVICES

Staff and students may use personally-owned devices at school for educational purposes and shall follow the same rules as other users of District electronic resources. Loss of network privileges also applies to personally-owned devices on the school network.

Those who choose to use their personally-owned device (laptop, tablet, iPad, iPod, etc) at school are responsible for the operation and security of the device. Personally owned devices shall NOT be supported by District personnel.

DISREGARD OF RULES

Individuals who violate District rules governing the use of District technology shall be denied further access. In appropriate cases, legal action may be taken.

Employees and students shall be subject to disciplinary action, up to and including termination (employees) and expulsion (students) for violating this policy and acceptable use rules and regulations established by the school or District.

RELATED POLICIES AND PROCEDURES:

08.2322; 09.14

Review/Revised:7/9/2019

Electronic Access/User Agreement Form

Staff Agreement

User's Name _____
Last Name *First Name* *Middle Initial*

User's Address _____ _____
City *State* *Zip Code*

Date of Birth _____ **Sex** ____

Phone Number _____ **School** _____

Employee's Job Title _____

As a user of the Taylor County School District's computer network, I hereby agree to comply with the District's Internet and electronic mail rules and to communicate over the network in a responsible manner while abiding by all relevant laws and restrictions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action and/or legal action may be taken.

User's Name (Please print) _____

_____ _____
User's Signature *Date*

Internal Use Only

Date Processed: _____
PROCESSED BY: _____