

## **TEACHER AND STUDENT OWNED DEVICES**

The District appreciates the fact that employees are willing to bring in personally owned devices to be used for school work and student use. However, several items must be addressed when connecting a non-KETS standard device to the District's network:

1. Security
2. Network stability
3. Liability for personal property
4. Virus protection
5. Repairs and upgrades

A student or staff member who brings privately owned devices to school are personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with the student/staff member. Loss or damage to the equipment is the responsibility of the individual.

## **TEACHER AND STUDENT OWNED DEVICES (CONTINUED)**

Software residing on privately owned devices must be personally owned. All computers must include anti-virus software.

District technicians will not service or repair any device not belonging to the District. No internal components belonging to the District shall be placed in any personal equipment, whether as enhancements, upgrades or replacements. No software or applications that are deemed by the District technology department to be for personal use will be supported by District level personnel. If personal software or an application interferes with the District network software or hardware, a technician may remove the personal software or application from the device. Any damage caused by use in the District is the responsibility of the owner.

Purchasing perishable supplies to be used in equipment not owned by the District is the owner's responsibility.

The District retains the right to determine where and when privately owned equipment may access the network. The student or staff member is responsible for the security of the equipment when it is not being used. The District will monitor all activity on privately owned devices. The District does not guarantee the privacy or security of any item stored on or transmitted by any privately owned devices.

The District retains the right to determine where and when privately owned equipment may access the network. The student/staff member is responsible for the security of the equipment when it is not being used. The District does not guarantee the privacy or security of any item stored on or transmitted by any privately owned devices.

A privately owned device can be connected to the District's network, including access to the Internet, under the following conditions:

1. The user has successfully completed a course in digital citizenship.
2. The connection has been approved and performed by the District technology department.
3. Use of the device adheres to the District Acceptable Use Policy.
4. File storage on the network from privately owned devices is limited to schoolwork only.

5. The individual must supply all necessary hardware/software and cabling to connect to the network.
6. Privately owned computing devices must be running virus detection software prior to accessing the network or Internet.

**TEACHER AND STUDENT OWNED DEVICES (CONTINUED)**

For privately owned devices being used in District facilities, the District reserves the right to:

1. Monitor all activity.
2. Make determinations on whether specific uses of the device are consistent with this policy.
3. Allot network use and monitor storage disk space utilized by such users.
4. Deem what is appropriate use.
5. Remove the user's access to the network and suspend the right to use the privately owned device in District facilities if at any time it is determined that the user is engaged in unauthorized activity or is violating this policy.

**RETENTION OF RECORDS FOR E-RATE PARTICIPANTS**

Following initial adoption, this policy and documentation of implementation shall be retained for at least five (5) years after the last day of service in a particular funding year.

**REFERENCES:**

KRS 156.675; 701 KAR 005:120; 16 KAR 1:020 KAR 001:020 (Code of Ethics)  
47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520  
Kentucky Education Technology System (KETS)

**RELATED POLICIES:**

03.1325/03.2325; 03.17/03.27  
04.32, 05.2, 05.22  
08.1353, 08.2321, 08.2322  
09.14, 09.421, 09.422, 09.425, 09.426

Adopted/Amended: 6/4/2013  
Order #: 15

**Access to Electronic Media**

(Acceptable Use)

**USE**

The Board supports reasonable access to various information formats for students, employees and the community and believes it is incumbent upon all users of electronic media and/or the AIS network 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 cyberbullying 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.

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.

**Access to Electronic Media**

(Acceptable Use)

**PERMISSION/AGREEMENT FORM**

A written parental request shall be required prior to a student's being granted independent 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 of minor students (those under 18 years of age) 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 (or the student who is at least 18 years old) must provide the Principal with a written request.

**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.
3. Guidelines may specify whether access to the site must be given to school/District technology staff.

**Access to Electronic Media**

(Acceptable Use)

**EMPLOYEE USE (CONTINUED)**

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.

**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.

**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.

**Access to Electronic Media**

(Acceptable Use)

**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**

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.

**TEACHER AND STUDENT OWNED DEVICES**

The District appreciates the fact that employees are willing to bring in personally owned devices to be used for school work and student use. However, several items must be addressed when connecting a non-KETS standard device to the District's network:

1. Security
2. Network stability
3. Liability for personal property
4. Virus protection
5. Repairs and upgrades

A student or staff member who brings privately owned devices to school are personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with the student/staff member. Loss or damage to the equipment is the responsibility of the individual.

**Access to Electronic Media**

(Acceptable Use)

**TEACHER AND STUDENT OWNED DEVICES (CONTINUED)**

Software residing on privately owned devices must be personally owned. All computers must include anti-virus software.

District technicians will not service or repair any device not belonging to the District. No internal components belonging to the District shall be placed in any personal equipment, whether as enhancements, upgrades or replacements. No software or applications that are deemed by the District technology department to be for personal use will be supported by District level personnel. If personal software or an application interferes with the District network software or hardware, a technician may remove the personal software or application from the device. Any damage caused by use in the District is the responsibility of the owner.

Purchasing perishable supplies to be used in equipment not owned by the District is the owner's responsibility.

The District retains the right to determine where and when privately owned equipment may access the network. The student or staff member is responsible for the security of the equipment when it is not being used. The District will monitor all activity on privately owned devices. The District does not guarantee the privacy or security of any item stored on or transmitted by any privately owned devices.

The District retains the right to determine where and when privately owned equipment may access the network. The student/staff member is responsible for the security of the equipment when it is not being used. The District does not guarantee the privacy or security of any item stored on or transmitted by any privately owned devices.

A privately owned device can be connected to the District's network, including access to the Internet, under the following conditions:

1. The user has successfully completed a course in digital citizenship.
2. The connection has been approved and performed by the District technology department.
3. Use of the device adheres to the District Acceptable Use Policy.
4. File storage on the network from privately owned devices is limited to schoolwork only.
5. The individual must supply all necessary hardware/software and cabling to connect to the network.
6. Privately owned computing devices must be running virus detection software prior to accessing the network or Internet.

**Access to Electronic Media**

(Acceptable Use)

**TEACHER AND STUDENT OWNED DEVICES (CONTINUED)**

For privately owned devices being used in District facilities, the District reserves the right to:

1. Monitor all activity.
2. Make determinations on whether specific uses of the device are consistent with this policy.
3. Allot network use and monitor storage disk space utilized by such users.
4. Deem what is appropriate use.
5. Remove the user's access to the network and suspend the right to use the privately owned device in District facilities if at any time it is determined that the user is engaged in unauthorized activity or is violating this policy.

**RETENTION OF RECORDS FOR E-RATE PARTICIPANTS**

Following initial adoption, this policy and documentation of implementation shall be retained for at least five (5) years after the last day of service in a particular funding year.

**REFERENCES:**

KRS 156.675; 701 KAR 005:120; 16 KAR 1:020 KAR 001:020 (Code of Ethics)  
47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520  
Kentucky Education Technology System (KETS)

**RELATED POLICIES:**

03.1325/03.2325; 03.17/03.27  
04.32, 05.2, 05.22  
08.1353, 08.2321, 08.2322  
09.14, 09.421, 09.422, 09.425, 09.426

Adopted/Amended: 6/4/2013  
Order #: 15