Formatted: Centered

Access to Electronic Media

STUDENT, STAFF AND COMMUNITY USE

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 student, staff and community member 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 use 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.

Access to Electronic Media

PERMISSION/AGREEMENT FORM FOR STUDENTS

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 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 Superintendent with a written request.

AGREEMENT FORM FOR STAFF AND COMMUNITY

A written request/agreement shall be required prior to the staff and/or community members being granted 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 and/or community user. 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~~shall~~ use electronic mail and other District technology resources to promote student learning and communications with the home and education-related entities. If those resources are used, they shall be used~~only~~ 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.

Access to Electronic Media

EMPLOYEE USE (CONTINUED)

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.
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.

Formatted: Space After: 4 pt

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.

STAFF/STUDENT OWNED MOBILE COMPUTING DEVICES

The District appreciates and welcomes the fact that staff and students are willing to bring personally owned computer equipment into the schools to be used for assignments and educational purposes. This policy applies to any use on District/School property.

Students in grades 5-12 may utilize the wireless guest network on a personally owned computing device with teacher permission if they have earned a Digital Drivers License which is not currently suspended. Students may not utilize a personal computing device that has been blocked from the network due to activity which violates the District Acceptable Use Policy.

Access to Electronic Media

STAFF/STUDENT OWNED MOBILE COMPUTING DEVICES (CONTINUED)

Students and/or employees who bring to school privately owned laptops or other mobile technology devices, including but not limited to, iPod Touch, iPad, etc., are responsible for the equipment. Further, use of such devices shall adhere to all guidelines in the District AUP and accompanying procedure(s).

DEFINITION

Any device that runs Palm OS, Windows CE, Pocket PC, Mac OS, or a like product is considered a computer. Any device that connects to the Internet via wireless connectivity is considered a computing device.

LIABILITY

A student or staff member who brings a privately owned laptop or other mobile technology device (e.g. iPod Touch, iPad, etc.) to school is personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with the student/staff member. Any damage to the equipment is the responsibility of the individual.

SOFTWARE AND HARDWARE

Software residing on privately owned computers must be personally owned. Licenses for Microsoft Windows 7 and Office2010 are available at affordable prices through the Kentucky Department of Education for all students and staff. All computer devices must include current anti-virus software.

No internal components belonging to the District shall be placed in any personal equipment, whether as enhancements, upgrades or replacements. If personal software or hardware interferes with the District network software or hardware, a technician may remove the computing device from the network. Any damage caused by use in the District is the responsibility of the owner.

TERMS AND CONDITIONS

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

- The connection has been approved and performed by the District technology department or a school technology resource teacher.
- Use of the computer adheres to the Breathitt County School District Acceptable Use Policy (AUP).
- All Internet traffic goes through the District proxy or filtering system as directed in Kentucky statutes (Senate Bill 230; 701 KAR 5:120).
- A USB flash drive is used to transfer files to the staff/student work station for network storage.

PRIVACY

All privately-owned computers attached and/or connected to the District's network are treated as the District's computers/devices for networking purposes. The District reserves the right to:

1. Monitor all activity and log network use.
2. Make determinations on whether specific uses of the computer are consistent with the District's AUP and the Schools' Code of Conduct/Handbook Policy.

Access to Electronic Media

PRIVACY (CONTINUED)

3. Install any additional management software or apply any permission/security policies to the equipment.
4. Remove the user's access to the network and suspend the right to use the privately owned computer in District/School facilities and on District/School property if at any time it is determined that the user is engaged in unauthorized activity or is violating the AUP.

The District does not guarantee the privacy or security of any item stored on or transmitted by any privately owned computers. Staff and students are NOT allowed to attach to any other wireless networks that may be unsecured in the neighborhood of the schools. Failure to comply with this policy will result in the termination of rights to use a wireless device in the schools.

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 to Electronic Media

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; KRS 365.732; KRS 365.734
701 KAR 5:120
16 KAR 1:020 (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
08.1353, 08.2322
09.14, 09.421, 09.422, 09.425, 09.426