

Access to Electronic Media

The Board supports reasonable access to various information formats for students, employees 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.

Certified employees are required to follow Board policy and administrative procedures and guidelines designed to provide guidance for access to electronic media. In addition, all staff members are required to sign a written agreement prior to being granted independent access to electronic media involving District technological resources. 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.

Because access to the Internet may expose users to items that are illegal, defamatory, inaccurate, or potentially offensive, we require all students under the age of eighteen (18) to submit a completed Parent Permission/User Agreement Form to the Principal/designee prior to access/use of District telecommunications and electronic information resources. All other users will be required to complete and submit a User Agreement Form prior to access/use.

RULES AND REGULATIONS

Access is a privilege—not a right. Users are responsible for appropriate behavior on school computer networks. Independent access to network service is given to individuals who agree to use resources in a responsible manner. Users are required to comply with District standards and to honor the access/usage agreements they have signed. Beyond clarification of user standards, the District is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network independently.

SUPERVISION OF STUDENT COMPUTER USE

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.

Teachers shall supervise all student computer use to ensure it is used for educational purposes and non-approved software, programs, and resources are not utilized.

Access to Electronic Media**SUPERVISION OF STUDENT COMPUTER USE (CONTINUED)**

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.

EMPLOYEE USE

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.
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.

Access to Electronic Media**EMPLOYEE USE (CONTINUED)**

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.

THE NETWORK

The Pikeville Independent School District provides students and staff with a service called the Network. The Network is a computer service, which includes the use of computers, servers, software, Internet and e-mail. These procedures also address the use of stand-alone computers, peripherals, telephone usage and other instructional technology equipment.

In addition to providing students and staff with the understanding and skills needed to use technology resources and telephone services in an appropriate manner, the Pikeville Independent School District:

- Reserves the right to monitor all activity on the Network, Internet and e-mail.
- Reserves the right to monitor computer use or lack of use.
- Reserves the right to deny access to the Network, Internet and e-mail to any individual.
- Shall establish procedures that will maximize the Network system security.
- Shall supervise student and staff use of the Network, Internet, e-mail, and telephones.

The standards for student and staff access to the Pikeville Independent School District Network are as follows:

- Network access throughout the District is to be used for instruction, research, school administration and reasonable, non-work related communications. District access is not to be used for private business.
- Instructional staff will select and guide students on the appropriate use of Internet and instructional software on the Network.
- The District will be responsible for supervising network use. Auditing procedures are in place to monitor access to the network. School and District proxy servers will be continually monitored and updated in accordance with the federal legislation, Children's Internet Protection Act (CIPA: 47 U.S.C. 254), KY Senate Bill 230, and KY KAR 5:120. However, the District cannot continually monitor every communication and network session for every student and staff member beyond the scope of supervision defined in the user agreement.
- 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.

Access to Electronic Media

THE NETWORK (CONTINUED)

- Internet access and supervision from outside the District premises is the responsibility of the parents and guardians of students.
- Student users should not reveal their full name and personal information (address, phone number, financial information, social security number, etc.) or establish relationships with “strangers” on the network, unless instructional staff has coordinated the communication.

TELEPHONE USAGE

- Telephone service is available primarily to provide two-way communications with school offices and for contact with parents.
- Staff will refrain from using telephones during instructional time.
- Students may use the telephones under staff supervision when there is a legitimate need such as calling parents to arrange transportation, delivery of medicine or clothes, or similar rare circumstances.
- Instruction time will not be interrupted to transfer calls except in emergencies.

All guidelines governing inappropriate language apply to telephone usage and procedures governing telephone usage also apply to District cellular phones and other wireless telecommunication systems.

COMPUTER USE GUIDELINES

When a student, teacher, or staff member at a Pikeville school accesses computers, computer systems, and computer networks owned or operated by the Pikeville Independent Schools, he or she assumes certain responsibilities and obligations. All access of this type is subject to school policies and to local, state, and federal laws. The school administration expects that student, faculty, and staff use of computers provided by the school will be ethical and will reflect academic honesty. Students, faculty and staff must demonstrate respect for intellectual property, ownership of data, system security mechanisms, and rights to privacy.

As a computer operator, you are expected to make appropriate use of computer resources provided by the Pikeville Independent Schools. You must:

- use computer resources only for authorized purposes following established procedures;
- be responsible for all activities on your assigned computer;
- access only files and data that are your own, which are publicly available, or to which you have been given authorized access;
- use only legal versions of copyrighted software;
- be considerate in your use of shared resources;
- abide by the acceptable Internet use policy.

Access to Electronic Media**COMPUTER USE GUIDELINES (CONTINUED)**

Computer operators must not make inappropriate use of computer resources provided by the Pikeville Independent Schools. Inappropriate actions include but are not limited to:

- using another person's login name or password;
- installing, downloading, or using any unauthorized software or hardware on any District computer system or Network;
- using another person's files, system, or data without permission;
- using computer programs to decode passwords or to access control information;
- attempting to circumvent or subvert system security measures;
- engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating viruses, damaging files, or disrupting service;
- making or using illegal copies or copyrighted software, storing such copies on school systems, or sending them over networks;
- using mail service to harass others;
- wasting computing resources, such as paper, by printing excessive copies;
- playing games across the network, including multi-user, web-embedded, or app-based games;
- violating the regulations of the Pikeville Independent Schools regarding appropriate use of the Internet.

The Pikeville Independent Schools considers any violation of appropriate use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information that may suggest that a person is using school computer systems inappropriately. Violators are subject to disciplinary action by school officials that may include loss of computer privileges and in- or out- of school suspension. Offenders may also be prosecuted under laws including, but not limited to, the Privacy Protection Act of 1974, the Computer Fraud and Abuse Act of 1986, the Computer Virus Eradication Act of 1989, and the Electronic Communications Privacy Act.

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.

INTERNET/EMAIL ACCESS

The Pikeville Independent School District provides access to the Internet for all students, faculty, and staff that is obtained through Kentucky's Public Education Network. Students must have permission from at least one of their parents or guardians to access the Internet at school.

The Pikeville Independent School District also provides email access to all faculty, staff, and students in grades 4-12. Students under the age of 18 must have parental permission to obtain an email account.

Access to Electronic Media**INTERNET/EMAIL ACCESS (CONTINUED)**

The use of an Internet account is a privilege, not a right, and inappropriate use will result in disciplinary action by school officials and/or cancellation of those privileges. A person's activities while using the Internet in any school must be in support of education and research and consistent with the educational objectives of the Pikeville Independent Schools. In addition, anyone accessing the Internet from a school site is responsible for all on-line activities that take place through the use of his or her account.

The following is a nonexhaustive list of activities that constitute unacceptable use of the Internet/Email:

- using impolite, abusive, or otherwise objectionable language in either public or private messages;
- placing unlawful information on the Internet;
- using the Internet illegally in ways that violate federal, state, or local laws or statutes;
- using the Internet at school for non-school related activities;
- sending messages that are likely to result in the loss of the recipient's work or systems;
- sending chain letters or pyramid schemes to lists or individuals, and any other types of use that would cause congestion of the Internet or otherwise interfere with the work of others;
- downloading, sharing, or using copyright protected media, including but not limited to music, video, and/or images in user-produced materials or internet content;
- using non-KETS and/or District assigned email, chat, or social media platforms;
- using the Internet for commercial purposes;
- using the Internet for political lobbying;
- changing any computer file that does not belong to the user;
- sending or receiving copyrighted materials without permission;
- knowingly giving one's password to others;
- using Internet access for sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the network;
- circumventing security measures, including web content filtering, on school or remote computers or networks (such as the use of Virtual Private Networks [VPN] applications on computers or mobile devices);
- attempting to gain access to another's resources, programs, or data;
- vandalizing, which is any malicious attempt to harm or destroy data or another user on the Internet, and includes the uploading or creation of computer viruses;
- falsifying one's identity to others while using the Internet.

Access to Electronic Media**DISCIPLINARY ACTION FOR INAPPROPRIATE USE**

- Student discipline for violation of any part of these procedures shall be based on the severity of the infraction.
- Student disciplinary action includes, but is not limited to, the loss of any or all computer privileges, termination of the user's account, removal from the class with a failing grade, and/or suspension or expulsion. Privileges will be reinstated at the discretion of the District's administrators.
- Discipline of staff may involve actions up to and including termination of employment.
- Parents, guardians and/or perpetrators may be billed for repair or replacement of District technology resources lost, stolen, damaged or vandalized while under their care.
- Illegal/criminal activities will be referred to the appropriate law enforcement agency.

All students and staff are required to sign the Acceptable Use Agreement Form. By signing the user agreement and/or parent permission form, the student or staff member has agreed to abide by Board policy governing access to technology resources. 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

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.

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.

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: 7/21/2020
 Order #: 1732