

## **Access to Electronic Media**

### **(Responsible Use Policy)**

The District provides access to and use of the Internet, email, and other District technology resources to its students and employees as part of the instructional process and to support the District's core values, mission, and vision. The Board supports this access and believes it is incumbent upon us 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 resources.

### **GENERAL STANDARDS FOR USERS**

Standards for users shall be included in the District's handbooks or other documents, which shall include specific guidelines for student, staff, and community member access to and use of electronic resources.

Access is a privilege—not a right. Users are responsible for good behavior on school computer networks. Independent access to network service is given to individuals who agree to act in a responsible manner. Users are required to comply with District standards and to honor the access/usage agreements.

The network is provided for users to conduct research and to communicate with others. During school hours, teachers 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.

District employees and students are expected to abide by the instructions set forth in the applicable Responsible Use Agreement if using and/or accessing District technology resources from home. This may include, but is not limited to: District owned computers, laptops, Chromebooks, tablets, or other devices; District provided cloud services, e-mail, and applications.

### **SAFETY PROCEDURES AND GUIDELINES**

The Superintendent/designee shall develop and implement appropriate procedures to provide guidance for access to global 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. Students who bring personal devices to school must use the school network to access the Internet. Use of mobile hotspots or personal data plans to access the Internet while at school is considered misuse.

**Access to Electronic Media**

(Responsible Use Policy)

**SAFETY PROCEDURES AND GUIDELINES (CONTINUED)**

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 students to inappropriate material on the Internet;
- Safety and security of students when they are using electronic mail, chat rooms, and other forms of direct electronic communications;
- Education of students about appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response;
- Preventing unauthorized access, including "hacking" and other unlawful activities by students online;
- Unauthorized disclosure, use and dissemination of personal information regarding students; and
- Restricting students' access to materials that are deemed obscene child pornography, or harmful to minors.

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.

**RESPONSIBLE USE AGREEMENT**

Because access to the Internet may expose users to items that are illegal, defamatory, inaccurate, or offensive, we require all students under the age of eighteen (18) to receive and honor a Responsible Use Agreement prior to access/use of District technology resources. All other users will also be required to receive and honor a Responsible Use Agreement.

The required student agreement (08.2323 AP.21) shall specify responsible uses of on-line behavior, access privileges, penalties for policy/procedural violations, and must be signed by the student and the parent/legal guardian of minor students (those under eighteen (18) years of age).

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 eighteen (18) years old) (or in case of an employee, the employee) must provide the Superintendent with a written request.

**Access to Electronic Media**

(Responsible Use Policy)

**EMPLOYEE USE**

Employees shall use electronic mail, technology resources, and network access only for purposes directly associated with work-related activities.

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 responsible for completing security awareness training and/or other training modules that are assigned to them.

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.

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/guardians concerning school-related activities.

District employees and activity sponsors may establish digital communication tools using District resources in accordance with guidelines to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction or when specific authorization is given by the Superintendent/designee for social networking accounts.

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**

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 this policy and responsibilities set forth in the Responsible Use Agreement.

**Access to Electronic Media**

(Responsible Use Policy)

**NO PRIVACY GUARANTEE**

The Superintendent/designee has the right to access information stored in any user directory, on a user's screen, or in District supported electronic communications. S/he may review files and communications to maintain system integrity and ensure that individuals are using the system responsibly. Users should have no expectation of privacy regarding the use of District property, technology-based devices, network, Internet access, files, and email.

**RESPONSIBLE USE VIOLATIONS**

Failure to sign or uphold the responsibilities listed in the student and/or employee Responsible Use Agreement form will be considered misuse. Misuse of District devices and/or networks may result in restricted access. Such misuse may also lead to disciplinary and/or legal action including suspension, expulsion, or termination.

**MAINTENANCE**

A maintenance program shall be developed by the Technology Director. The maintenance program shall include provisions which will minimize "down-time" on network file servers.

**RESPONSIBILITY FOR DAMAGES**

The District makes no guarantees about the quality of the services provided and is not liable for any claims, losses, damages, costs, or other obligations arising from use of the network, District accounts, or equipment. Users are responsible for any charges incurred while using District devices and/or network including repair or replacement for District resources lost, stolen, damaged, or vandalized while under their care. The District also denies any liability for the accuracy or quality of the information obtained through user access. Any statement accessible online is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Students under the age of eighteen (18) should only access District network accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the student's use outside of school.

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 (08.2322).

**Access to Electronic Media**

(Responsible Use Policy)

**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 District shall establish a process to prevent and monitor the District's educational technology from 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 students and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by students, harmful to students;
2. Maintaining and securing a usage log;
3. Monitoring online activities of students; and
4. The District will take necessary measures to secure the network against potential cyber security threats. This may include blocking access to District applications, including but not limited to email, data management and reporting tools, and other web applications.

**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; 8.1353, 08.2322  
09.14, 09.421, 09.422, 09.425, 09.426; 09.4261; 10.5

Adopted/Amended: 6/17/2021  
Order #: 10917