



BULLITT COUNTY PUBLIC SCHOOLS
DEPARTMENT OF TECHNOLOGY

KEVIN FUGATE, DIRECTOR & CIO

SARAH SMITH, ADMINISTRATIVE ASSISTANT

SARAH CARNES, INVENTORY SPECIALIST

ANDREW HOBBS, NETWORK ADMINISTRATOR

M E M O

03.03.2026

TO: Jesse Bacon, Superintendent

FR: Kevin Fugate, Director of Technology & CIO

RE: Acceptable Use Policy Update

Due to the recent integration of emerging technologies, such as artificial intelligence, into the educational environment, a revision to the BCPS Acceptable Use Policy (AUP) is required to safeguard both students and staff.

We have also incorporated details regarding KRS 160.145 (also known as SB 181), which restricts staff from using messaging services not officially approved by the district for communication with students.

This revised policy has been reviewed and approved by our district's legal counsel. This constitutes the first reading, and we will request final approval at the next regular board meeting. Thank you!

BULLITT COUNTY PUBLIC SCHOOLS IS AN EQUAL EDUCATION AND EMPLOYMENT INSTITUTION

Access to Electronic Media

(Acceptable Use Policy)

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.

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 the 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 to 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;
- Safe and responsible use of emerging technologies such as artificial intelligence (AI);
 - Protecting personally identifiable information and privacy when using AI applications
 - Being aware of potential biases in AI algorithms and interpreting outputs critically
 - Modeling the safe, appropriate, and responsible use of AI, avoiding misuse or harm.
- 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 FORM

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

Access to Electronic Media

(Acceptable Use Policy)

PERMISSION/AGREEMENT FORM (CONTINUED)

The required permission/agreement form, which shall specify acceptable uses, rules of online 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.

By signing this agreement, parents/guardians also give consent for BCPS to act as an agent for the parent in the collection of information within the school context as required by the Children's Online Privacy Protection Act (COPPA). This includes granting permission for the student to use District-approved third-party online web applications and services for educational purposes, which may require the creation of individual student accounts and the minimal collection of personal identifying information (such as name, address, etc).

SUPERVISION OF STUDENT TECHNOLOGY USE

Teachers and others whose duties include classroom management and/or student supervision shall sign an Acceptable Use Policy agreement acknowledging responsibility for exercising reasonable supervision of student access to the Internet, electronic mail, and emerging technologies, including artificial intelligence. District internet content filtering devices, district-provided online monitoring tools, and AI-powered monitoring tools shall not be treated as a substitute for classroom management and direct monitoring of student online activities.

Teachers shall not direct or advise students accessing school computing and communications networks to use third-party email systems or AI tools that bypass Kentucky Department of Education or Bullitt County Board of Education-approved messaging systems.

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, internet access 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:

CURRICULUM AND INSTRUCTION

08.2323
(CONTINUED)

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

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 the release of student information under state and federal law.

Teachers and school staff must use approved, traceable district communication systems to interact with students, as state legislation and district policy prohibit private electronic communication outside of these official platforms without prior written parental consent.

This is in accordance with [KRS 160.145](#), also known as SB 181.

All teacher to student communication must adhere to the Kentucky Teacher Code of Ethics ([016 KAR 1:010](#)) and focus strictly on professional, or educational purposes. Under KRS 160.145, staff are prohibited from connecting with students on personal social media; however, they may maintain separate professional pages for school activities, but are still prohibited from messaging students on any social media platform unless given permission by the parent/guardian. Using phone, text, or email for personal

discussions with students is forbidden without explicit parental consent. Finally, per KRS 620.030, staff must report any evidence of neglect or potential harm—including information discovered online—to the proper authorities immediately.

CURRICULUM AND INSTRUCTION 08.2323

(CONTINUED)

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

All employees shall be subject to disciplinary action if their conduct relating to the 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.

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 website 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.

CURRICULUM AND INSTRUCTION

08.2323
(CONTINUED)

AUDIT OF USE

Users with network access shall not utilize District resources to establish and/or access electronic mail accounts through third-party providers or any other nonstandard electronic mail system, unless permission is granted by the District Technology Coordinator/CIO.

Access to Electronic Media

(Acceptable Use Policy)

AUDIT OF USE (CONTINUED)

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 the 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.

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 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; 45 C.F.R. 54.520
Kentucky Education Technology System (KETS)
[KRS 160.145](#)

RELATED POLICIES:

03.1325/03.2325; 03.17/03.27
08.1353; 08.2322
09.14, 09.421, 09.422, 09.425, 09.426

Adopted/Amended: 7/28/2014
Order #: 22