LEGAL: HB 67 AMENDS KRS 160.145 ADDING ADDITIONAL INDIVIDUALS FOR REPORTING PURPOSES. THIS BILL CONTAINS AN EMERGENCY CLAUSE AND IS IN EFFECT AS OF APRIL 13, 2026. •
FINANCIAL IMPLICATIONS: NONE ANTICIPATED

CURRICULUM AND INSTRUCTION 08.2323

Formatted: Centered

Access to Electronic Media

(Acceptable/Responsible 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 and authorized communication system(s). 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.

Guidelines and procedures should encourage details on how the District implements and facilitates digital learning tools and portable/mobile technologies to foster ubiquitous access for staff and students, emphasizing always-on, everywhere digital opportunity and empowering Districts and schools to fully understand digital access beyond the campus. With such District implemented resources, the guidelines for acceptable and responsible use shall still apply, regardless of the time, place, and means of utilization.

The District shall support teacher efforts in taking ownership of digital citizenship skills and educating their students in the same skills to foster a responsible, safe, secure, and empowered digital learning environment. 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, District-managed systems and accounts, and personal devices that are permitted to access the District's network, shall be implemented that effectively address the following, regardless of the time, place, and means of utilization:

Formatted: Space After: 0 pt

- 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,- direct messaging platforms, social media, and other forms of direct electronic communication~~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.

Access to Electronic Media

(Acceptable/Responsible Use Policy)

SAFETY PROCEDURES AND GUIDELINES (CONTINUED)

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

All applicable procedures and guidelines resulting from this AUP/RUP shall be readily available and for use by students, parents/guardians, faculty, staff and other to whom access is granted. A written parental or legal guardian request shall be required to opt-out of or rescind access to electronic media involving District technological resources. Or if appliable procedures require, a written parental request may be required to prior to the student being granted independent access to electronic media involving District technological resources. This document shall be kept on file as a legal, binding document.

The required permission/agreement materials, which shall specify acceptable uses, rules of online behavior, access privileges, and penalties for policy/procedural violations, must be acknowledged by the parent or legal guardian of minor students (those under 18 years of age) and also by the student. In order to opt-out, 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.

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 authentication credentials. Employees shall enroll in and use multi-factor authentication (MFA) for all district-assigned accounts and systems where multi-factor authentication (MFA) is available. Multi-factor authentication (MFA) shall not be disabled or bypassed except with written authorization from the Director of Technology for documented operational necessity.

Formatted: ksba normal

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.

- Infiinite Campus Messenger
- Canvas

Formatted: Space After: 0 pt

Access to Electronic Media

(Acceptable/Responsible Use Policy)

EMPLOYEE USE (CONTINUED)

In accordance with KRS 160.145, the Board designates the following traceable communication systems~~, to be the exclusive means~~ for District employees and qualified school volunteers to communicate electronically with students enrolled in the District..

- Apptegy
- District Email
- Edgenuity
- District Google Workspace (Docs/Sheets/Slides/Forms/Classroom/Meets)
- GoGuardian/Peardeck
- Kami

Formatted: Space After: 0 pt

No other networking and communications systems, other than those listed within policy, shall be used to facilitate communication between District employees or volunteers and students. ~~The Principal of each school shall provide parents written or electronic notification within the first ten (10) days of the school year of each electronic school notification and communication program designated within the traceable communication system. The notification shall include instructions for parents to access and review communications sent through each electronic school notification and communication program. See policy 08.2324 for complete details and guidelines.~~

A District employee or qualified school volunteer~~, unless authorized,~~ shall not engage in unauthorized electronic communication.~~ communicate electronically with a student~~:

~~1. Outside of the traceable communication system designated by the Board; or~~

~~2. Through an unauthorized electronic communication program or application.~~

~~This shall not restrict any electronic communications between a student and his or her family member who is a District employee or volunteer.~~

Formatted: Indent: Left: 0.25"

Networking, communication systems, and other options offering the ability to communicate directly with students may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.~~ in accordance with Policy 08.2324.~~

Students may only be invited or granted access to Board approved traceable electronic communications systems, including social media platforms and other digital communication sites, if the District has verified that the system meets acceptable data privacy standards and includes appropriate protections for student information. Furthermore, the students must meet the platform's minimum age requirements before being granted access or invited to access.

Staff members shall not use or create personal social networking accounts to which they communicate directly with or invite students to be friends. However, this prohibition shall not restrict any social media communication between a student and his or her family member who is a District Employee or Volunteer.

See policy 08.2324 for complete details and guidelines regarding Traceable Communications.

Access to Electronic Media

(Acceptable/Responsible Use Policy)

EMPLOYEE CONDUCT AND REPORTING REQUIREMENTS FOR TECHNOLOGY USE

All employees and volunteers are subject to disciplinary action if their conduct relating to the use of technology or online resources violates this policy or any other applicable statutory, regulatory or policy provisions governing employee conduct. This includes, but is not limited to, unauthorized electronic communications. Employees shall not store personally identifiable information, education records, or other District data in personal cloud storage services (including personal Goggle Drive, iCloud, Dropbox, Microsoft OneDrive, or similar services not managed by the District.) All district data shall be stored in District-managed systems. The requirement applies regardless of the device used.

Formatted: ksba normal

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 the confidentiality of student information. Any conduct in violation of this Code – particularly involving technology or online resources - must be reported to the Education Professional Standards Board (EPSB) as required by law and may result in disciplinary action up to and including termination.

~~**REPORTING PROCEDURES – POLICY 08.2324**~~

~~A District employee or volunteer who receives a report alleging that another District employee or volunteer has engaged in unauthorized electronic communication must immediately notify the appropriate authority:~~

~~1. If the subject of the report is a staff member, notify the Principal.~~

~~1. If the subject is the Principal, notify the Superintendent.~~

~~2. If the subject is the Superintendent, notify the Commissioner of Education and the Chair of the local Board.~~

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which District technology resources (including internet access, computer equipment, software, and information access systems) may 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.

Access to Electronic Media

(Acceptable/Responsible Use Policy)

DIGITAL CITIZENSHIP AND RESPONSIBLE USE

All District technology users shall demonstrate safe, savvy, and social digital citizenship skills by practicing respectful, responsible, and ethical use of technology. The District will ensure comprehensive instruction on digital citizenship, focusing on the nine (9) elements of digital citizenship: Digital Access; Digital Commerce; Digital Communication & Collaboration; Digital Fluency; Digital Etiquette; Digital Law; Digital Rights and Responsibilities; Digital Health and Welfare; and Digital Security & Privacy, as well as cyberbullying awareness and response strategies, are provided. All digital citizenship instruction shall align with the Kentucky Academic Standards for Technology and be reviewed regularly to reflect current best practices and emerging technologies. The District shall support efforts to instill digital citizenship skills in students to foster a responsible, safe, and empowered digital learning environment. District-provided technology resources shall be used in a manner that upholds the integrity, security, and privacy of district systems and supports educational goals regardless of the time, place, and means of utilization.

DISREGARD OF RULES

Individuals who opt-out of required responsible 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.

EMERGING TECHNOLOGIES

The District shall establish and maintain procedures that address the safe, secure and responsible uses of emerging technologies, including, but not limited to, artificial intelligence (AI) and AI-enhanced or generative AI features. These procedures shall be reviewed and updated regularly to ensure alignment with current technological advancements, fostering a proactive approach while emphasizing safeguards for student safety, data privacy, and ethical practices. Such procedures will support innovative strategies while addressing potential risks and maintaining the confidence of district stakeholders. Additionally, procedures will address the responsible use of these emerging technologies, including appropriate and inappropriate uses of AI (e.g., for inspiration vs. cheating, plagiarism).

Access to Electronic Media

(Acceptable/Responsible Use Policy)

EMERGING TECHNOLOGIES (CONTINUED)

Notwithstanding any procedure adopted under this section, no employee or student shall input, upload, or otherwise submit personally identifiable information or education records into any artificial intelligence tool or generative AI platform that has not been approved by the District through the vendor evaluation process. This prohibition applies to both personally owned AI tools and any AI-enabled feature with an otherwise approved platform that has been specifically reviewed and approved.

Formatted: ksba normal

Formatted: policytext, Left, Space After: 0 pt

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 social media (unless authorized by a teacher for instructional purposes) and 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. For instructional purposes, age/grade-level appropriateness and meets traceable/inspectable guidelines set forth in this and related policies;
2. Utilizing the latest available filtering technology to ensure that social media is not made available to students, unless authorized by a teacher for instructional purposes;
3. Maintaining and securing a usage log; and
4. Monitoring online activities of both minors and adults using District-owned or managed systems, regardless of the time, place, and means of utilization.

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 160.145; 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; 47 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516
15-ORD-190

Access to Electronic Media

(Acceptable/Responsible Use Policy)

RELATED POLICIES:

03.13214/03.23214
03.1325/03.2325
03.17/03.27
08.1353; 08.2322; 08.2324
09.14; 09.421; 09.422; 09.425; 09.426; 09.4261
10.5

Formatted: Centered

Employee Reports of Criminal Activity

To promote the safety and well-being of students, the District requires employees to make reports required by state law in a timely manner. Supervisors and administrators shall inform employees of the following required reporting duties:

KRS 158.155

Any school employee who knows or has reasonable cause to believe that a person has made threats or plans of violence which are intended to target a school or students or who knows that a firearm is present on school property in violation of KRS 527.070 shall immediately cause a report to be made to the District's law enforcement agency and to either the local law enforcement agency or to the Kentucky State Police.

Any school employee shall immediately report to the District's law enforcement agency and to either the local law enforcement agency or to the Kentucky State Police any act which the employee has a reasonable cause to believe has occurred on school property or at a school-sponsored or sanctioned event involving:

a. Intentional physical injury, or intentional attempt to cause physical injury, as defined in KRS 500.080, to any school employee;

~~a.~~b. Intentional ~~A~~assault resulting in serious physical injury, as defined in KRS 500.080;

~~b.~~c. A sexual offense;

~~c.~~d. Kidnapping;

~~d.~~e. Assault with the use of a weapon;

~~e.~~f. Possession of a firearm or deadly weapon in violation of the law;

~~f.~~g. The use, possession, or sale of a controlled substance in violation of the law; or

~~g.~~**h.** Intentional or wanton ~~D~~damage to property **causing a pecuniary loss of five hundred dollars ($500) or more**.

Any school employee who receives information from a student or other person of conduct which is required to be reported shall report the conduct to the District's law enforcement agency and to either the local law enforcement agency or to the Kentucky State Police, unless the school employee has cause to believe a student's disability interfered with his or her ability to conform to the Student Code of Conduct.

~~A District that has created their own law enforcement agency shall designate a local law enforcement agency not created by the District to receive reporting information from the District's law enforcement agency. The District's law enforcement agency shall file a weekly report for the preceding week identifying all reports received under KRS 158.155.~~

Formatted: ksba normal

Formatted: ksba normal

Formatted: ksba normal

Formatted: ksba normal

Formatted: ksba normal

Formatted: ksba normal

Formatted: Default Paragraph Font, Font: Bold

Formatted: ksba normal

Formatted: Default Paragraph Font, Font: Bold

Formatted: ksba normal

Employee Reports of Criminal Activity

KRS 158.156

Any employee of a school or a local board of education who knows or has reasonable cause to believe that a school student has been the victim of a violation of any felony offense specified in KRS Chapter 508 committed by another student while on school premises, on school-sponsored transportation, or at a school-sponsored event shall immediately cause an oral or written report to be made to the Principal of the school attended by the victim. The Principal shall notify the parents, legal guardians, or other persons exercising custodial control or supervision of the student when the student is involved in an incident reportable under this section. The Principal shall file a written report with the local school board and the local law enforcement agency or the Department of Kentucky State Police or the county attorney within forty-eight (48) hours of the original report.

KRS 160.380

When an allegation of abusive conduct, as defined in KRS 160.380, is made against a District employee to another District employee, the District employee in receipt of the allegation, whether communicated in writing, electronically, or orally, shall report the allegation to the Principal and in accordance with KRS 620.030. The Principal shall document the allegation in writing and notify the Superintendent/designee. An investigation of the allegation shall be conducted by the District until it is completed and shall not end prior to completion due to the employee transferring positions within the District or leaving the District, unless directed by the Cabinet for Health and Family Services or law enforcement officials to cease the investigation.

KRS 209A.100

Upon the request of a victim, school personnel shall report an act of domestic violence and abuse or dating violence and abuse to a law enforcement officer. School personnel shall discuss the report with the victim prior to contacting a law enforcement officer.

KRS 209A.110

School personnel shall report to a law enforcement officer when s/he has a belief that the death of a victim with who s/he has had a professional interaction is related to domestic violence and abuse or dating violence and abuse.

KRS 620.030

Any person who knows or has reasonable cause to believe that a child is dependent, neglected, or abused, or is a victim of human trafficking, or is a victim of female genital mutilation, shall immediately cause an oral or written report to be made to a local law enforcement agency or the Department of Kentucky State Police; the cabinet or its designated representative; the Commonwealth's Attorney or the County Attorney; by telephone or otherwise. Any supervisor who receives from an employee a report of suspected dependency, neglect, or abuse shall promptly make a report to the proper authorities for investigation.

Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold
Formatted: ksba normal, Font: Not Bold

Employee Reports of Criminal Activity

REFERENCES:

KRS 158.155; KRS 158.156; KRS 160.380
KRS 209A.100; KRS 209A.110
KRS 508.125; KRS 525.070; KRS 525.080; KRS 527.070; KRS 527.080
KRS 620.030

RELATED POLICIES:

03.13251; 03.23251; 03.13253; 03.23253
05.48
09.227; 09.422; 09.423; 09.425; 09.426; 09.438