Access to Electronic Media
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

The ~~Board supports reasonable access to various information formats for~~ District provides access to and use of the Internet, email and other District technology resources to its students~~,~~ and employees ~~and the community~~ 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 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 ~~they have signed~~.

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

SAFETY PROCEDURES AND GUIDELINES

The Superintendent/designee 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 technology~~ical~~ 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.

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 material~~matter~~ on the Internet ~~and World Wide Web~~;

Access to Electronic Media
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

SAFETY PROCEDURES AND GUIDELINES (CONTINUED)

- Safety and security of minors when they are using electronic mail, chat rooms, and other forms of direct electronic communications;
- Education of minors 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 minors online;
- Unauthorized disclosure, use and dissemination of personal information regarding minors; and
- Restricting minor's 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~~PERMISSION/~~ AGREEMENT ~~FORM~~

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 ~~submit a completed~~receive a Responsible Use Agreement ~~Form to the Principal/designee~~ prior to access/use of District technology resources. All other users will also be required to ~~complete and~~honor ~~submit a~~ Responsible Use Agreement ~~Form~~.~~A written parental request shall be required prior to the student being granted independent access to electronic media involving District technological resources~~.

The required student ~~permission/~~agreement form (08.2323 AP.21), ~~which~~ shall specify ~~acceptable~~responsible uses, ~~rules~~ of on-line behavior, access privileges, and penalties for policy/procedural violations~~;~~ and must be signed by the student and 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) (or in case of an employee, the employee) must provide the Superintendent with a written request.

EMPLOYEE USE

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

Access to Electronic Media
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

EMPLOYEE USE (CONTINUED)

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 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 concerning school-related activities.

~~District employees and activity sponsors may not set up social networking accounts using District resources or create such accounts associated with a school/District location or organization unless specific authorization is given by the Superintendent/designee.~~

District employees and activity sponsors may ~~set up authorized blogs~~ establish digital communication tools using District resources in accordance with~~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 or when specific authorization is given by the Superintendent/designee for social networking accounts.

~~In order for District employees and activity sponsors to utilize a District approved blog or authorized social networking account 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, an authorized site will be established by the Superintendent's designee and specific permissions will be set for the appropriate school personnel to conduct and monitor blogging activities.~~

~~3. Once the blog site or authorized social networking account has been created, and permissions set, the sponsoring staff member is responsible for the following:~~

~~a. Monitoring and managing the site(s) 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
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

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.

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 this Policy and the responsibilities set forth in the Responsible Use Agreement Form~~the Superintendent/designee~~.

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 insure 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~~DISREGARD OF RULES~~

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, termination, or criminal prosecution by government authorities as appropriate.

~~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.~~

Access to Electronic Media
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

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 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 minor's use outside of school.

~~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 (08.2322).

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~~Superintendent/designee~~ shall establish a process to prevent and monitor~~determine whether~~ the District's educational technology ~~is~~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 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.
4. The District will take all 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.

Access to Electronic Media
(Responsible Use Policy)
~~(Acceptable Use Policy)~~

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 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

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

Employee Responsible Use Policy Agreement ~~Form~~

EMPLOYEE RESPONSIBILITY

Employees supervising students using technology are to be vigilant in order to ensure students are meeting the provision outlined in the Responsible Use Policy (RUP) 08.2323.

DIGITAL CITIZENSHIP

- All employees are responsible for modeling, actively practicing, and advocating for positive digital citizenship.
- Employees using classroom technology are explicitly required to teach students about positive digital citizenship.
- What employees do and post online must not disrupt school activities or compromise school safety and security, including, but not limited to, personal social media accounts.
- Employees must model and actively practice personal responsibility for lifelong learning.

PRIVACY

- Employees shall not share personally identifiable information about students ~~and~~or employees as defined in KRS 61.931 including, but not limited to, names, home addresses, birthdates, telephone numbers, student ID numbers and employee numbers.
- Transfer of student information shall be only through approved District information systems.
- Employees must be aware of privacy settings on websites that they visit.
- Employees will abide by all laws, the District RUP, and all District security policies.
- Devices reported to the District as lost or stolen are subject to verification of internal network information including locating the device using IP addresses, GPS location services, and screenshots.

PASSWORDS

- Under no circumstances are District passwords to be shared with others, including other District staff and students.
- Log out of unattended equipment and accounts in order to maintain privacy and security.

PROFESSIONAL LANGUAGE

- Use professional language in all work-related communications including email, social media posts, audio recordings, conferencing, and artistic works.

CYBERBULLYING

- Bullying in any form, including cyberbullying, is unacceptable both in and out of school.
- Report all cases of bullying to the site administrator or other authority.

INAPPROPRIATE MATERIAL

- Do not seek out, display, or circulate material that is hate speech, sexually explicit, or violent while under employment with Henderson County Schools.
- Exceptions for questionable material may be made in an appropriate educational context with permission of the Principal.
- The use of the District network for illegal or commercial purposes is strictly forbidden.
- The use of the District network or equipment shall not be used to endorse any political candidate.
- Transmitting large files that are unrelated to District business and disruptive to the District network is prohibited.

Responsible Use Policy Agreement ~~Form~~

EMPLOYEE RESPONSIBILITY (CONTINUED)

SECURITY

- Use District-approved email for all school-related purposes and while on school property.
- All users are responsible for respecting and maintaining the security of District technology resources and networks.
- Do not use the District network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.
- Do not try to bypass security settings and filters, including through the use of proxy servers.
- Do not install or use illegal software or files, including unauthorized software or apps, on any District computers, tablets, Chromebooks, smartphones, or new technologies.

EQUIPMENT AND NETWORK SAFETY

- Take all reasonable precautions when handling District equipment.
- Use caution when downloading files or opening emails as attachments could contain viruses or malware.
- Vandalism in any form is prohibited and must be reported to the appropriate administrator and/or information technology personnel.
- Users are responsible for damages to and loss of equipment assigned to them by the District.

COPYRIGHT

- While there are fair use exemptions (http://www.copyright.gov/fls/fl102.html), all users must respect intellectual property.
- Follow all copyright guidelines (http://copyright.gov/title17/) when using the work of others.
- Do not download illegally obtained music, software, apps, and other works.

CONSEQUENCES FOR IRRESPONSIBLE USE

Failure to uphold the responsibilities listed above is misuse. Misuse of District devices and networks may result in restricted access or account cancellation. Such misuse may also lead to disciplinary and/or legal action against employees, including personnel action and/or criminal prosecution by government authorities.

DISCLAIMER

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. 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.

~~After having read the above information, sign below and return to your administrator or other designated supervisor.~~

~~***I have read, understand, and agree to the Responsible Use Policy (RUP) of Henderson County Schools.***~~

~~School/Office:~~ _____

~~Employee Name:~~ _____ ~~Employee Number:~~ _____

~~Employee Signature:~~ _____ ~~Date:~~ _____

~~*Please return this form to your supervisor or administrator to be kept on file. It is required for all employees that will be using a computer network and/or Internet access.*~~

Student Responsible Use Policy Agreement ~~Form~~

STUDENT RESPONSIBILITY

INSTRUCTIONS

Read each section ~~and sign below~~. Students are to review each section with a parent or guardian ~~and get their signature below~~. ~~Return to your teacher or other designated school site personnel.~~

~~By signing this agreement, you~~ Users acknowledge that ~~you~~ they understand the following:

I am responsible for practicing positive digital citizenship.

- I will advocate for and practice positive digital citizenship, including appropriate behavior on all electronic communications, including new technology.
- I will be honest in all digital communication.
- I understand that what I do and post online must not disrupt school activities or compromise school safety and security.
- I will demonstrate personal responsibility for lifelong learning.

I am responsible for keeping personal information private.

- I will not share personally identifiable information about myself or others including, but not limited to, names, home addresses, telephone numbers, birth dates, or visuals such as pictures, videos, and drawings.
- I will not meet anyone in person that I have met only on the Internet.
- I will be aware of privacy settings on websites that I visit.
- I will abide by all laws, the District Responsible Use Policy, and all District security policies.
- I understand that if a device is reported to the District as lost or stolen, it may be located using IP addresses, GPS location services, and screenshots.

I am responsible for my passwords and my actions on District accounts.

- I will not share any school or District usernames and passwords with anyone.
- I will not access the account information of others.
- I will log out of unattended equipment and accounts in order to maintain privacy and security.

I am responsible for my verbal, written, and artistic expression.

- I will use school appropriate language in all electronic communications, including email, social media posts, audio recordings, video conferencing, and artistic works.

I am responsible for treating others with respect and dignity.

- I will not send and/or distribute hateful, discriminatory, or harassing digital communications, or engage in sexting.
- I understand that bullying in any form (in or out of school) including cyberbullying, is unacceptable.
- Should I become aware of cyberbullying taking place, I will notify a counselor, teacher or administrator immediately.

I am responsible for accessing only educational content when using District technology.

- I will use only school approved email and communication systems while on school property.
- I will not seek out, display, or circulate material that is hate speech, sexually explicit, or violent.
- I understand that any exceptions must be approved by a teacher or administrator as part of a school assignment.
- I understand that the use of the District network for illegal, commercial purposes, or to support a political candidate is strictly forbidden.

Student Responsible Use Policy Agreement ~~Form~~

STUDENT RESPONSIBILITY (CONTINUED)

I am responsible for respecting and maintaining the security of District devices and networks.

- I will not try to get around security settings and filters, including through the use of proxy servers to access websites blocked by the District.
- I will not install or use illegal software or files, including copyright protected materials, unauthorized software, or apps on any District devices.
- I know that I am not to use a personal data plan / mobile hotspot at school to access the Internet, including enabling access on District devices.
- I will not use the District network or devices to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.

I am responsible for taking all reasonable care when handling District equipment.

- I understand that vandalism in any form is prohibited.
- I will report any known or suspected acts of vandalism to the appropriate authority.
- I will respect my and others' use and access to District equipment.
- I understand that I am responsible for damages to and loss of equipment assigned to me by the District.

I am responsible for respecting the works of others.

- I will follow all copyright (http://copyright.gov/title17/) guidelines.
- I will not copy the work of others and represent it as my own and I will properly cite all sources.
- I will not download illegally obtained music, software, apps, and other works.

SUMMARY

All users are responsible for practicing positive digital citizenship. Positive digital citizenship includes appropriate behavior and contributions on websites, social media, discussion boards, media sharing sites and all other electronic communications, including new technology. It is important to be honest in all digital communications without disclosing sensitive personal information. What District community members do and post online must not disrupt school activities or otherwise compromise individual and school community safety and security.

~~*I have read, understand, and agree to the Responsible Use Policy of Henderson County Schools.*~~

~~School:~~ _____ ~~Date:~~ _____

~~Student Name:~~ _____ ~~Student Signature:~~ _____

~~Parent/Legal Guardian Name:~~ _____

~~Parent/Legal Guardian Signature:~~ _____

~~HR/Advisory Teacher Name:~~ _____ ~~Room Number:~~ _____

~~*Please return this form to the school where it will be kept on file. It is required for all students that will be using a computer network and/or Internet access.*~~