

Access to Electronic Media

ELECTRONIC MAIL/INTERNET

The District offers students, staff, and members of the community access to the District's computer network for electronic mail and Internet. All staff and students grade 3 and above will have a District email account. Because access to the Internet may expose users to items that are illegal, obscene, defamatory, inaccurate, or offensive, the District shall require all users to complete and submit an Electronic Access/User Agreement Form (08.2323 AP. 21) to the Principal/designee prior to access/use.

Except in cases involving students who are at least eighteen (18) years of age and have no legal guardian, parents/guardians may request that the school/District:

- Provide access so that the parent may examine the contents of their child(ren)'s email files;
- Terminate their child(ren)'s individual email account and/or Internet access; and
- Provide alternative activities for their child(ren) that do not require Internet access.

Parents/guardians wishing to challenge information accessed via the District's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

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 to electronic media 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. Beyond clarification of user standards, the District is not responsible for restricting, monitoring, or controlling the communications of individuals utilizing the network independently.

The network is provided for users to conduct research and to communicate with others. Within reason, freedom of speech and access to information will be honored. 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.

NO PRIVACY GUARANTEE

The Superintendent/designee has the right to access information stored in any user directory, on the current user screen, or in electronic mail. S/he may review files and communications to maintain system integrity and insure that individuals are using the system responsibly. Users should not expect files stored on District servers or through District provided or sponsored technology services, to be private.

Access to Electronic Media**RULES AND REGULATIONS**

Violations of the Acceptable Use Policy include, but are not limited to, the following:

1. Violating State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
2. Sending or displaying offensive messages or pictures, including those that involve:
 - Profanity or obscenity; or
 - Harassing or intimidating communications.
3. Damaging computer systems, computer networks, or school/District websites.
4. Violating copyright laws, including illegal copying of commercial software and/or other protected material.
5. Using another user's password, "hacking" or gaining unauthorized access to computers or computer systems, or attempting to gain such unauthorized access.
6. Trespassing in another user's folder, work, or files.
7. Intentionally wasting limited resources including downloading of software or malware to District hardware.
8. Using the network for commercial purposes, excessive personal use, financial gain or any illegal activity.
9. Using technology resources to bully, threaten or attack a staff member or student or to access and/or set up unauthorized blogs and online journals, including, but not limited to Facebook.com, Twitter.com, Snapchat or other emerging social media sites.
10. Connecting to networks other than District provided wireless networks is prohibited while on school property.
11. The BCPS network may not be used to remotely connect to computers or other devices outside of our network without expressed written permission from the District Technology Coordinator.
12. Installing software or other devices to BCPS owned hardware in order to gain remote access to the BCPS network is prohibited unless approved by the District Technology Coordinator or CIO.
13. It is not permissible to connect any device to District-owned computers/network in order to illegally capture or download data.

Any Internet activity, whether posted from school or another location, that materially or substantially disrupts the educational process may result in disciplinary and/or legal action.

Additional rules and regulations may be found in District Code of Student Behavior and Discipline handbook and/or other documents. Violations of these rules and regulations may result in loss of access/usage as well as other disciplinary or legal action.

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 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, this is often referred to as Digital Citizenship, or Digital Driver's License (DDL).

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.

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

An Electronic Access/User Agreement Form 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 (referred to as AUP), which shall specify acceptable uses, rules of on-line 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.

CHECKOUT OF SCHOOL OWNED ELECTRONIC DEVICES

Electronic devices may be made available for student checkout but shall be the responsibility of the person to whom the device is issued and be subject to all provisions set out in the policy and related procedures. In addition, a signed AUP form must be on file at the school or District level before an electronic device is issued to a student. Participants in the District 1:1 Program (Access 24) shall refer to the Access 24 Plan and Technology Responsible Use Expectations (TRUE) for guidelines and other information.

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 Internet and electronic mail. District internet content filtering devices shall not be treated as a substitute for classroom management and monitoring of student internet use.

Teachers shall not direct or advise students accessing school computing and communications networks to use third party email systems (Yahoo, Mail.com, or personal Gmail/Office 365 accounts) other than the Kentucky Education Technology System standard email system.

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 shall treat District passwords and student data with the utmost security.

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.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

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.

Any form of communication with students must be consistent with 16 KAR 1:010, Standards for Certified School Personnel (the Kentucky Teacher Code of Ethics).

Staff members are prohibited from extending invitations to or accepting invitations from students on any "personal social networking sites" that does not serve a legitimate professional, or educational purpose unless the student's parent/guardian has knowledge of the communication and gives specific permission for same. Staff members may create a classroom "fan or professional" page to communicate with students and parents information directly relating to classroom and school activities. The staff member's "fan or professional" page shall be separate from his/her personal networking page. Employees creating such "fan or professional" pages are responsible for all content posted on the website. Any social networking site, blog or other emerging technology used to communicate with students and parents shall include the disclaimer "This site is not monitored on a 24/7 basis". ALL school personnel are required by KRS 620.030 to report to the proper authorities either orally or in writing any knowledge of a student who is in danger of being harmed by himself/herself or another or any student who is neglected. This would include information gathered from a social networking site.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

Employees shall not use any form of communications (phone/cell, phone/texting, or email) to discuss items of a “personal” nature with students that does not serve a legitimate professional, or educational purpose, unless the student’s parent/guardian has knowledge of the communication and gives specific permission for same.

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 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 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.

Access to Electronic Media

(Acceptable Use Policy)

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.

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 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 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:

03.133214/03.23214; 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

Electronic Access/User Agreement Form

STUDENT FORM

Student Name _____			_____			_____		
<i>Last Name</i>			<i>First Name</i>			<i>Middle Initial</i>		
Address _____								
			<i>City</i>			<i>State</i>		<i>Zip Code</i>
Age _____		Date of Birth _____		Sex: (Circle One) M or F		Phone Number _____		
Grade _____			School _____			Homeroom/Classroom _____		

As a user of the Bullitt County District’s computer network, I hereby agree to comply with the District’s Internet and electronic mail rules and to communicate over the network in a responsible manner while abiding by all relevant laws and restrictions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action and/or legal action may be taken.

Student Name (Please print) _____

Student Signature *Date*

Students will be supervised by a staff member, while on school grounds, during any Internet access.

As the parent or legal guardian of the student signing above, I grant permission for my child to access networked computer services such as the Internet. I understand that my child will be supervised while selecting, researching, sharing or exploring electronic information and media. However, I realize that some objectionable materials could be inadvertently encountered.

CONSENT FOR USE

By signing this form, you hereby accept and agree that your child’s rights to use the electronic resource provided by the District and the Kentucky Department of Education are subject to the terms and conditions set forth in District policy/procedure. Please also be advised that data stored in relation to such services is managed by the District pursuant to policy 08.2323 and accompanying procedures. You also understand that the email address provided to your child can also be used to access other electronic services or technologies that may or may not be sponsored by the District, which provide features such as online storage, online communications and collaborations, and instant messaging. Use of those services is subject to either standard consumer terms of use or a standard consent model. Data stored in those systems, where applicable, may be managed pursuant to the agreement between KDE and designated service providers or between the end user and the service provider. Before your child can use online services, he/she must accept the Service Agreement and, in certain cases, obtain your consent.

Name of Parent/Guardian (Please print) _____

Signature of Parent/Guardian *Date*

Email Address: _____

Daytime Phone Number: _____ Evening Phone Number: _____

NOTE: Federal law requires the District to monitor online activities of minors.

Electronic Access/User Agreement Form

EMPLOYEE/STUDENT TEACHER FORM

The following agreement form is to be distributed to all Bullitt County School District employees including substitute and student teachers. A signed agreement form must be on file at the school or assigned building for each employee or student teacher who wishes to use the Network or Internet. The building Principal/Designee will retain all forms. By signing the user agreement the employee or student teacher has agreed to abide by Board policies governing access to technology resources and employee use.

___ **YES**, I have read the Bullitt County School District Staff/Student Teacher Acceptable Use Policy. I understand and will abide by the stated terms and conditions. Should I commit any violation, my access privileges may be revoked and disciplinary action, up to and including termination of employment or university disciplinary action, shall be taken. Furthermore, appropriate legal action may be taken. I understand that if I engage in unauthorized conduct that results in liability, I will assume full responsibility for that liability and release and hold the District harmless for any consequences that result from my conduct.

If students are assigned to my care, I agree to direct students to acceptable Network/Internet resources and monitor their use at all times. I agree to enforce the Student Acceptable Use Policy with students. I agree to instruct students on acceptable use of the Network, Internet and proper Network/Internet/Email etiquette.

BCPS EMPLOYEE RESPONSIBILITY (INCLUDING SUBSTITUTE AND STUDENT TEACHERS)

Name (Please print): _____

Location _____

Job Title: _____

Signature: _____ Date: _____

If the user is a Student Teacher, the following information must be completed.

Supervising Teacher: _____ Signature: _____

(By signing this form, you agree, as Supervising Teacher, to monitor this Student Teacher's use of the network and email as stated in the District Acceptable Use Policy.)

Ending Date of entire Student Teaching Assignment: _____

(NOTE: If the student teacher is doing two (2) sessions at two (2) different schools, please put the ending date from the last teaching assignment.)

(The student teacher's account will be terminated at the end of the entire Student Teaching Assignment.)

Student Teacher Signature: _____ Date: _____

NOTE: Student teachers will not be added to a school email distribution list. School-wide emails will need to be forwarded from your Supervising Teacher.