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. 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 Parent Permission/User Agreement Form to the Principal/designee prior to access/use. All other users will be required to complete and submit a User Agreement Form.

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 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 District network is built and maintained with state and federal funds and, as such, most information stored within the network is considered public domain and may be subject to Open Records and Freedom of Information Act requests. Therefore, there is no guaranteed right to privacy for any user of the District Network.

Access to Electronic Media

NO PRIVACY GUARANTEE (CONTINUED)

Users should not expect any file stored on electronic systems within the District network or through District provided or sponsored technology services, to be private. Designated school/District staff have the right to access files and data stored on District servers, on the current user screen, and within the electronic mail system. Designated school/District staff may review files and communications to ensure the integrity and responsible use of District network resources.

NETWORK, INTERNET AND ELECTRONIC MESSAGING REGULATIONS

Users of the District Network will be given an account in order to access the District's computer network after agreeing to the terms of the District's Acceptable Use Policy (AUP) and related procedures. All users must submit a signed copy of the AUP to signify their agreement to abide by these policies/procedures. For minor students, a parent or guardian must sign the AUP form authorizing, and approving student use of network resources, including computer systems, Internet, and e-mail. This access is a privilege and not a right. Any user found to be in violation of the AUP and/or procedures outlined within this document may have these privileges suspended or revoked. Permission must be granted at least once for all users in the District and will remain in effect until such time as the user leaves the District or until permission is revoked by parent and/or guardian request. Such a request may be made at any time throughout the school year. Parent/guardian permission requests must be made in writing to the appropriate school's office. A signed copy of the AUP form will be retained on file in a central location.

APPROPRIATE USE OF NETWORK RESOURCES

In order to provide for user security, legal compliance, and the security of data, the following guidelines must be adhered to by all users of network resources:

I. **ACCESS TO INAPPROPRIATE MATERIAL** – in accordance with 701 KAR 5:120 Prevention of Objectionable Material Transmitted to Schools via Computer.

   Access of materials deemed as inappropriate by any user, including but not limited to, sexually explicit and/or obscene material is strictly prohibited. The District utilizes Internet filtering technology in order to limit access to such sites and materials. However, no system is perfect and students and teachers must be the first line of defense against access to this type of content. All internet traffic is logged and archived. If a faculty member suspects that a student has accessed an inappropriate website, a request can be made of the District technology staff to retrieve the logs for a particular student for a given period of time. The local administrative staff at the school will then evaluate the data and take the appropriate action. This action may include suspension of the student's internet access up to prohibition on use for the remainder of the school year. In the case of a faculty or staff member who is thought to have accessed inappropriate content, usage logs for that particular individual will be retrieved and submitted to the Superintendent for review.

Access to Electronic Media

II. **INTERNET SAFETY AND SECURITY -** in accordance with 701 KAR 5:120 Prevention of Objectionable Material Transmitted to Schools via Computer.

The safety of students is of utmost importance to the District. Likewise, the security and safety of faculty and staff and District data is also an extremely high priority. Student access of unauthorized social websites from the District network is expressly forbidden. Student access to electronic chat rooms, Internet Relay Chat, Skype, etc., is not permitted without strict faculty supervision. These types of sites are filtered by our Internet filtering system.

The only e-mail system that may be accessed via the District's network is the Kentucky Department of Education's approved system. Access to any other e-mail system via our network is strictly prohibited. Furthermore the use of e-mail, Internet, and other network resources is for educational use only. Teachers, staff, and parents may request a site be blocked. Subject to review by District network administrators and school staff, sites can be added to a blacklist to prevent student access.

III. **INTERNET SAFETY AND SECURITY UNAUTHORIZED ACCESS –** in accordance with KRS 434.840-860 Unlawful Access to a Computer

Unlawful access to a computer is a felony. Access of the District network and/or a school owned computer may only be permitted with a user's personal log-in and password. A user may not reveal their password to anyone nor may they use another user's password to access a District computer or network. The use of any hardware or software in an attempt to gain access to a computer and/or network, obtain another user's password, or interfere with the flow of information on the network is strictly prohibited. The downloading and use of Port Scanners, hacking software, etc., is strictly prohibited unless authorized in an IT class and monitored by a faculty member. Any user found in violation of this statute may, at minimum, lose their network/computer privileges and/ or be brought up on criminal charges.

IV. Misuse of Computer Information - in accordance with KRS 434.855 Misuse of Computer Information

Any user who accesses information of a sensitive or confidential nature without proper authorization, including software and/or records, or assists another in doing the same, is in violation of KRS 434.855 Misuse of Computer Information. Examples of this type of information include, but are not limited to, Infinite Campus for student records and data, MUNIS and CPA for financial records. Gaining access to these types of information and redistributing to others, changing information (such as student grades or attendance records) constitutes violation of this statute. Any user in violation of this statue may, at minimum, lose their network/computer privileges and/or be brought up on criminal charges. It is further understood that unauthorized personnel should not be allowed to see, copy, or disseminate any data of a private nature. In the event of a breach of data security, the network administrator will be notified and action will be taken as necessary to prevent further data loss. (See 01.61 AP.11.)

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. Access or use of any e-mail system other than the state approved and provided KETS mail system (Outlook and Exchange) - for example: Hotmail, Gmail, Yahoo Mail, etc.);
3. Sending or displaying offensive audio, video, photographic, or print materials;
4. Transmitting or using obscene or profane language, sexually explicit, or pornographic material;
5. Harassing, intimidating, bullying, or attacking others;
6. Damaging computer systems, computer networks, school/District websites, or other technology resources both internally or externally;
7. Introducing viruses, spyware, adware, or malware of any type onto the network;
8. Violating copyright laws, including illegal copying of commercial software and/or other protected material;
9. Allowing another user access to a computer or network via your account;
10. Trespassing in another user's folder, work, or files;
11. Using District technology resources to maintain any unauthorized blogs, online journals, or social networking sites;
12. Using the network for commercial or personal purposes such as:
    a. running a private business
    b. conducting activities related to a non-school related club or organization
    c. soliciting or obtaining money, property, or services for personal or private sector use
    d. promoting political or religious purposes
    e. engaging in gambling or gaming
13. Using the network or messaging system to forward chain emails, spam, or non-educational materials; or
14. 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 MySpace.com, Facebook.com or Xanga.com.

Additional rules and regulations may be found in District handbooks 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.

Review/Revised:7/17/12