Access to Electronic Media for Adults and Students

Erlanger/Elsmere Schools
Acceptable Use Policy for Access to Electronic Media

The Erlanger/Elsmere School District ("District") provides students and certain adults with a service hereinafter referred to as **the Network**. The Network is a computer service, which includes the use of servers, software, Internet and Email. This Adult Acceptable Use Policy (the "Policy") addresses the use of the Network and also the use of technology resources provided by the District, including desktop computers, laptop computers, tablets, "smart" phones, and other instructional technology equipment ("Electronic Instructional Devices").

GENERAL PRINCIPLES FOR BOTH ADULTS AND STUDENTS

The standards for student and staff access to the Network are:

1. Internet access for students must be agreed upon by the parents/guardians of students.
2. Network access throughout the District is to be used for educational purposes, instruction, research, and school administration only. Network access is not to be used for personal activity, private business, illegal activity, political activity, or accessing sexually-oriented or other inappropriate material, including material promoting drugs, alcohol, tobacco, or any other illegal activity (including hacking).
3. The District will monitor Network use. Auditing procedures are in place to monitor access to and use of the Network. However, the District cannot continually monitor every communication and Network session for every student and staff member. Although the district does implement filters to decrease the risk, users should be warned that some material accessible via the Network may contain items and information that are illegal, defamatory, inaccurate, or sexually explicit, or otherwise potentially offensive to some people.
4. District supplied electronic mail is not private. District personnel and others who operate the Network do have access to all Email, and Email usage is monitored. Messages relating to or in support of illegal activities may be reported to the authorities. Messages relating to or in support of activities which violate the school discipline code shall be reported to the school administration. Messages which indicate that a student may be in danger or may harm himself/herself or another person shall also be reported to the school administration and other appropriate authorities. Employees should be aware that Internet access logs and email content may be open to inspection and are subject to open records laws.
5. Students and employees are prohibited from using District resources to establish or access Internet Email accounts through third party providers. Only Kentucky Education Technology Systems Email can be used.

ELECTRONIC INSTRUCTIONAL DEVICE REGULATIONS

As a technology resource operator, you are expected to make appropriate use of technology resources and Electronic Instructional Devices. The regulations listed below apply to the Network, Internet, Email, instant messaging, social networking, and Electronic Instructional Devices. You shall:

1. Be responsible for all activities on your assigned Electronic Instructional Device;
2. Access only files and data that are your own, which are publicly available, or to which you have been given authorized access;
3. Use only legal versions of copyrighted software;
4. Be considerate in your use of shared resources; in other words, don't "hog" system resources by playing non-instructional online videos, playing games on the Internet, or doing anything else that would unnecessarily slow the network and interfere with its use by others.

Electronic Instructional Device operators must not make inappropriate use of resources provided by the District. The following are non-exhaustive actions that are considered inappropriate:

- Using home ISP-provided email, or any other unauthorized Email service;
- Using another person's login name or password;
- Installing, making copies, distributing or using any unlicensed software or hardware on the Network or on any District Owned Electronic Instructional Device;
- Engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating viruses, damaging files, disrupting service, or deleting or modifying programs;
- Committing plagiarism, fraud, misrepresentation, or other dishonest acts.
- Using harassing, abusive, or otherwise objectionable language in either public or private messages;
- Using the Network illegally in ways that violate federal, state, or local laws or statutes;
- Using the Network for commercial purposes;
- Using the Network for political lobbying;
- Knowingly giving one's password to others or allowing others to use your account;

Access to Electronic Media for Adults and Students

- Circumventing security measures on school or remote computers or networks;
- Deleting electronic communications that are required for legal document retention;
- Posting or exchanging personally identifiable student information on the Network without permission from District personnel;
- Transmitting obscene, abusive, or sexually explicit language or materials;

All of the above apply to district-owned technology used regardless of location. In other words, a user utilizing a district-owned laptop at his or her own house is bound by these guidelines in the same way that he or she would be inside of the district Network.

DISREGARD OF RULES

The District considers any violation of this Policy to be a serious offense and reserves the right to copy and examine any files or information that may suggest that a person is using technology resources inappropriately. Violators are subject to disciplinary action by school officials that may include loss of computer privileges and/or expulsion for students and termination for staff. Offenders may also be prosecuted under laws including, but not limited to, the Privacy Protection Act of 1974, the Computer Fraud and Abuse Act of 1986, and the Computer Virus Act.

RESPONSIBILITY FOR DAMAGES

Individuals shall reimburse the Board for repair/replacement of District property lost, stolen, damaged, or vandalized while under their care. Students or staff members who deface or otherwise make unauthorized changes to a District web site shall be subject to disciplinary action.

USE OF PERSONALLY OWNED DEVICES ON THE DISTRICT NETWORK (i.e. "Bring Your Own Device" or "BYOD")

Staff and students (with parental permission) are allowed to connect personally owned devices to the district Network. There is a separate policy for BYOD usage, and staff and students are directed to it for further guidelines.

ADDITIONAL GUIDELINES FOR STUDENTS

SOCIAL NETWORKING REGULATIONS

An online social network is a web site or mobile app with the goal of building a social community of individuals who share a common interest and/or activity. Popular social networking sites include Facebook.com, Twitter.com, and the social networking tools built into the district-supplied email system.

- Social networking sites such as those mentioned above may only be accessed if the following three criteria are met: 1) Access to such sites is for educational use. 2) You are directly supervised by a teacher or other staff member who is aware of and approves of your attempt to access such a site. 3) Such sites are **not** blocked by the district technology department.
- Students shall not reveal their name or Personally Identifiable Information to, or establish relationships on the Internet unless a parent or teacher has coordinated the communication.
- Students who utilize social networking for educational purposes shall be familiar with privacy options on the social networking site, and shall set those options to limit access to personal information to "friends" only.
- Students and parents shall be aware, however, that privacy options alone can never fully protect personal information. If a student shares personal information with "friends," those friends may share that information with others. With this in mind, students shall carefully consider what information is posted online.
- Photos posted on social networking sites used for educational purposes shall NOT contain other students. Permission, either spoken or in writing, should be granted from any adults before posting their pictures.
- Teachers and other adult staff have been advised NOT to "friend" students on social networking sites using the same account used for personal social networking. Students are given the same advice. Remember that teachers are ethically and legally bound to report any activity in which a student may be breaking the law or may be in danger of hurting him/herself or others.
- You shall not utilize social networking sites to harass or bully others.

Access to Electronic Media for Adults and Students

ADDITIONAL GUIDELINES FOR ADULT USERS

- Adults should not permit nor encourage students to reveal their full name and personal information, such as address, phone number, financial information, social security number, etc. ("Personally Identifiable Information") via the network.
- Adults should not themselves upload student Personally Identifiable Information into any cloud-based software system without written permission from the Superintendent or his designee.
- Adults should not permit students to establish relationships on the Network, unless instructional staff has coordinated the communication.
- Staff will not reveal a student's full name or post a picture of the student or the student's work on the Network with Personally Identifiable Information unless the parent has given prior written consent.
- Employees should use discretion when accessing and potentially making electronic and/or paper copies of sensitive data. This includes storing Personally Identifiable Information on personal or school-issued mobile devices.
- The content of any District web page is the responsibility of the staff member who hosts the page.

ELECTRONIC COMMUNICATION REGULATIONS, INCLUDING EMAIL, INSTANT MESSAGING, AND SOCIAL NETWORKING

Employees are encouraged to use electronic mail and other District technology resources to promote student learning and communication with the home and other education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

District employees and activity sponsors may set up blogs and other social networking accounts using District resources and following this Policy to promote communication with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

In order for District employees and activity sponsors to utilize a social networking site (Facebook, Twitter, etc.) using District-owned or District-provided technology resources 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 (i.e. usernames and passwords) 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/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. ALL school personnel should remember that they are required by KRS 620.030 to report to the proper authorities in writing *any* knowledge of a student who is in danger of being harmed by him/herself or another, or any student who is neglected. This would include information gathered from a social networking site (e.g. a student in his/her "status" states that he/she is contemplating suicide).

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 as required by law and may form the basis for disciplinary action up to and including termination.

Access to Electronic Media for Adults and Students

TEACHER AND STAFF 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. Teachers shall not direct nor advise students accessing school computing and communications networks to use electronic mail systems other than the Kentucky Education Technology System standard email system.

In the same way that a teacher or library media specialist provides various levels of guidance to students visiting a library, the teacher/staff member supervising student use will want to structure various levels of Internet access depending upon age, grade level, or student performance. For instance:

1) Very young children should not be provided with unsupervised access to the Network. At the lower grade levels, an Internet or Email session may be best conducted with small groups and always supervised by a teacher or someone the teacher has designated.
2) Children in middle school, who are familiar with the Network, and generally demonstrate good conduct, might be provided with limited independent access in a location where the session can be monitored.
3) In the upper grades, those students with good standing who have proven their ability to be responsible Network users might be provided with independent, unsupervised access for research purposes.

NOTE: The following paragraph is required by the Kentucky Department of Education to be included on all district Acceptable Use Policy forms, and is necessary to give users access to the state-provided online communication system.

By signing this form, you herby accept and agree that your child's rights to use the electronic resources provided by the District and/or the Kentucky Department of Education (KDE) 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 e-mail 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 are 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.

NOTE: The following paragraph is required in order to allow students under the age of 13 to utilize district-approved, third party websites that require parental permission.

The Erlanger-Elsmere School District partners with several third-party vendors to provide educational technologies over the Internet. The district cares about the protection of student personal data, and all approved vendors have agreed to protect the security of student personal data and to use the data for educational purposes only (i.e. They do not sell student information to advertisers or to others). Some of these partner sites, though, require students under the age of 13 to receive parent or guardian consent prior to using.

By signing this form, you are giving consent for the district and its approved third party vendors to provide these services to your child.

A complete list of these services is online at http://www.erlanger.kyschools.us/Content2/PII.

Review/Revised: 7/12/2018