Kenton County School District
Acceptable Use Guidelines

The Kenton County 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. These guidelines address the use of the Network and also the use of technology resources provided by the District, including desktop computers, laptop computers, net books, PDA's, word processors, peripheral telephone usage, and other instructional technology equipment ("Electronic Instructional Devices").

In addition to providing students and staff with the understanding and skills needed to use technology resources and telephone services in an appropriate manner, the Kenton County School District reserves the right to monitor all activity on the Network, including Internet, Email, and instant messaging. Furthermore the District:

1. Reserves the right to monitor computer use or lack of use.
2. Reserves the right to deny access to the Network, including Internet, Email, and instant messaging to any individual.
3. Shall establish procedures that will maximize the Network system security.

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

1. 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, persuasive political activity, or accessing sexually-oriented or other inappropriate material (e.g. material promoting drugs, alcohol, tobacco, illegal activity, etc.)
2. 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. Additionally, the content of the Network includes many statements and opinions. These expressed statements and opinions are not those of the district.
4. Internet access for students must be agreed upon by the parents/guardians of students.
5. 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").
6. Adults should not permit students to establish relationships on the Network, unless instructional staff has coordinated the communication.
7. 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.
8. The content of any District web page is the responsibility of the sponsoring staff member who hosts the page.
9. Network access is only permissible by District staff, District administration, and District students.

TELEPHONE USAGE

- Telephone service is available primarily to provide two-way communications with the school office and for contact with parents.
- Staff will refrain from using telephones during instructional time.
- Students may use the telephones under staff supervision when there is a legitimate need such as calling parents to arrange transportation, delivery of medicine or clothes, or similar rare circumstances. Instructional time will not be interrupted to transfer calls except in emergencies.

All standards and regulations contained within this Policy governing inappropriate language apply to telephone usage. The regulations governing telephone usage also apply to District cellular phones and other district wireless telecommunication systems.

ELECTRONIC INSTRUCTIONAL DEVICE
When a district student, teacher, or staff member accesses the Network or an Electronic Instructional Device owned or operated by the district, he/she assumes certain responsibilities and obligations. All access of this type is subject to school policies and to local, state, and federal laws. The school administration expects that student, faculty, and staff use of technology resources provided by the school will be ethical and will reflect academic honesty. Students, faculty and staff must demonstrate respect for intellectual property, ownership of data, and system security mechanisms.

As a technology resource operator, you are expected to make appropriate use of technology resources and Electronic Instructional Devices provided by the District. The guidelines listed below apply to the Network, Internet, Email, instant messaging communications, 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;

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

- Using Google Gmail, or any other unauthorized Email service;
- Using another person's login name or password;
- Installing or using any unlicensed software or hardware on the Network or on any District Owned Electronic Instructional Device;
- Using another person's files, system, or data without permission;
- Using computer programs to decode passwords, to access control information, or access unauthorized computers or networks;
- Attempting to circumvent or subvert system security measures;
- 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;
- Making or using illegal copies of copyrighted software, storing such copies on school systems, or sending them over the Network;
- Using Email or other Network services to harass others;
- Wasting technology resources, such as paper, by printing excessive copies;
- Playing non-educational games or using the Network for other non-educational purposes;
- Committing plagiarism, fraud, misrepresentation, or other dishonest acts.

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.

INTERNET ACCESS GUIDELINES

The District provides access to the Internet for all students, faculty, and staff. This access is obtained through the Kentucky Educational Network. The use of a Network account is a privilege, not a right, and inappropriate use will result in disciplinary action up to and including termination and/or cancellation of Network privileges. A person's activities while using the Network in any school must be in support of education and research and consistent with the educational objectives of the District. In addition, anyone accessing the Network from a school site is responsible for all on-line activities that take place through the use of his or her account. When using another organization's networks or computing resources, you must comply with the rules appropriate for that network.

The following is a non-exhaustive list of prohibited activities that constitute unacceptable use of the Network, whether that use is initiated from school or any other site:

1. Using harassing, abusive, or otherwise objectionable language in either public or private messages;
2. Placing unlawful information on the Network;
3. Using the Network illegally in ways that violate federal, state, or local laws or statutes;
4. Sending messages that are likely to result in the loss of the recipient work or systems;
5. Sending chain letters or pyramid schemes to lists or individuals and any other types of use that would cause congestion of the Network or otherwise interfere with the work of others;
6. Using the Network for commercial purposes;
7. Using the Network for persuasive political lobbying;
8. Changing any computer file or record that does not belong to the user or that the user should not access;
9. Sending or receiving copyrighted materials without permission;
10. Knowingly giving one's password to others or allowing others to use your account;
11. Using Network access for sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the Network;
12. Circumventing security measures on school or remote computers or networks;
13. Attempting to gain access to another's resources, programs, or data;
14. Any malicious attempt to harm or destroy data or another user on the Network and includes the uploading or creation of harmful files;

15. Falsifying one's identity to others while using the Network;
16. Deleting electronic communications that are required for legal document retention;
17. Logging on with the use of another person's password or account;
18. Posting or exchanging personally identifiable student information on the Network without permission from District personnel;
19. Transmitting obscene, abusive, or sexually explicit language;
20. Creating or sharing computer viruses;
21. Interfering with, sabotaging, or vandalizing the computer hardware or software of others, including that belonging to the District;
22. Obtaining software from or putting software onto the Network without first obtaining written pre-approval from school personnel;
23. Violating any copyright or software license;
24. Engaging in any form of illegal activity, including fraud or forgery or any other misrepresentation;
25. Promoting any illegal conduct or the use of drugs, alcohol, or tobacco;

ELECTRONIC COMMUNICATION GUIDELINES, 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 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 this Policy to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication, e-mail 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 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/Principal/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. 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/her self or another or any student who is neglected. This would include information gathered from a social networking site.

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.

Students and employees of the District are prohibited from using District resources to establish and/or access Internet Email accounts through third party providers. Only Kentucky Education Technology Systems Email can be used.

- Be polite. Do not write or send abusive, degrading, or defamatory messages to others.

- You shall not use Email for communications that are not directly related to instruction or sanctioned school activities.
- You shall not swear, use vulgarities, obscenities, or any other inappropriate language.
- You shall not send or attach anything containing lewd, vulgar, pornographic, obscene, or sexually explicit material.
- You shall not access, copy or transmit another user's messages without permission.
- You shall not send electronic messages using another person's name or account.
- You shall not send electronic messages anonymously.
- You shall ensure that you have kept a copy of all documents required for legal document retention.

The 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 will be reported to the school administration. Messages which indicate that a student may be in danger or may harm himself/herself or another person will also be reported to the school administration and other appropriate authorities.

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 or advice students accessing school computing and communications networks to use electronic mail systems other than the Kentucky Education Technology System standard email system.

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.

REFERENCES:

KRS 156.675; 47.U.S.C.§ 254; 701 KAR 5:120
16 KAR 1:020 (Code of Ethics)
Public Law 110-385, Broadband Data Improvement Act/Protecting Children in the 21st Century Act.
Kentucky Education Technology System (KETS)

RELATED POLICIES:

03.17/03.27
03.1325/03.2325
08.1353; 08.2322
09.14; 09.421; 09.422; 09.425; 09.426