Access to Electronic Media

(Staff Acceptable Use Policy)

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.

PURPOSE AND INTENT

The Russell County Board of Education has adopted an Acceptable Use Policy to guide access to information in electronic media, to information technology, and to networks. The purposes of this policy are: to educate; to provide protection against violations of privacy, misuse of state resources, and inappropriate or destructive behaviors which occur as a result of employee access to electronic information sources; and, to ensure that the technology resources of the District are dedicated to improving service and raising productivity. Each employee of the Russell County Board of Education shall sign an Acceptable Use Policy Statement acknowledging their awareness of the policy and their understanding of individual responsibility related to policy compliance.

SCOPE

This policy includes a description of technical resources available to employees, related laws and policies, issues for additional consideration, and recommendations for maximizing the use of Russell County School District hardware, software, and information. The policy extends to: computer hardware and peripherals; software; network services such as electronic mail and Internet; network access; storage devices; databases, files and other repositories of information in electronic form. This policy applies to both onsite and remote access.

APPLICABILITY AND RESPONSIBILITY FOR COMPLIANCE

This policy applies to all employees of the Russell County Board of Education, including all personnel serving under contract or memorandum of agreement.

RESPONSIBILITY FOR COMPLIANCE

Members of Russell County School District are responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance is expected, and that intentional inappropriate use may result in disciplinary action. Each individual is responsible for their own actions and the actions of those they knowingly permit to use assigned resources and passwords.

INFORMATION TECHNOLOGY RESOURCES

Identifying Examples of Appropriate and Inappropriate Use

Decisions about appropriate and inappropriate use of information technologies can be based on the same criteria which guide decisions about use of other public agency assets. For example:

- Public resources may not be used for private business or personal gain;

Access to Electronic Media

(Staff Acceptable Use Policy)

INFORMATION TECHNOLOGY RESOURCES (CONTINUED)

- Copyrights must be respected and authorship must be appropriately acknowledged;
- No social networking sites allowed, including but not limited to, Face book, MySpace or Twitter; and
- Vandalism, theft, prying, and willful destruction will not be tolerated.

Electronic records are also subject to the provisions of the law related to records scheduling, retention, and disposal.

Employees must be aware that electronic mail logs, the content of electronic mail, Internet access logs and the content of Internet sessions may be subject to inspection under the open records laws and are not necessarily private. Employees should remember that electronic mail, Internet access, and other resources are provided for the purpose of carrying out assigned work. Be advised that email can be monitored at any time.

There are numerous federal laws and regulations governing access to information managed by the Department of Education and the local school districts. The Appropriate Use Policy also assumes knowledge of and adherence to federal requirements. Information about managing the security of student records in electronic form may be found in "Program Review 95-KETS-152, Security of Student Records in the Kentucky Education Technology System."

EMAIL AND OTHER ELECTRONIC RESOURCES

Parents must accept and agree that their 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. They also are advised that data stored in relation to such services is managed by the District pursuant to this policy and accompanying procedures. They must understand that the e-mail address provided to their 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 a student can use online services, he/she must accept the service agreement and, in certain cases, obtain parental consent.

PORNOGRAPHY, SEXUAL HARASSMENT, AND OTHER OBJECTIONABLE MATERIALS:

The introduction of Internet access and the ease with which electronic images and files may be transported increases the risk that pornography and other objectionable materials will be copied, created, or distributed through the use of public agency information resources. Pornography viewed by others inadvertently may constitute grounds for sexual harassment. Objectionable materials would include information from hate groups, information posted to harass or threaten, etc.

Access to Electronic Media

(Staff Acceptable Use Policy)

PORNOGRAPHY, SEXUAL HARASSMENT, AND OTHER OBJECTIONABLE MATERIALS: (CONT.)

It is a violation of the Acceptable Use Policy to send, receive, store, create, display, or transmit pornography and other objectionable materials using District resources. This includes, but is not limited to:

- Placing such materials on or retrieving them from a public agency fileservers, hard drive, or other storage media;
- Sending or receiving pornography and objectionable materials through the network;
- Using public agency resources and/or network access to download from or post such materials to personally-owned devices.

COPYRIGHT

Most software and much of the information posted on the Internet are copyrighted. Before software can be loaded on a computer or fileserver, the District or school must have the legal right to install that particular version of the software. The software license will specify whether the rights purchased are for a single user on a single workstation, for multiple users, or for multiple workstations. Software may not be copied or shared outside the provisions of the agreement with the software publisher. Violations of software licensing agreements may constitute serious infractions of federal law and the violator may be subject to civil and/or criminal penalties.

Do not:

- Copy software without authorization from the publisher or copyright holder;
- Use software for which you do have proof of legal right;
    i) Copy information or programs from the Internet and re-use or distribute it without authorship and source;
    ii) Assume that you can load the older version of software on another workstation when you install a software upgrade.

GUIDELINES

The user is responsible for the security of his/her user account. If passwords are distributed to others, the user is responsible for the actions of those to who access is given. If the user leaves the workstation unattended with applications open, the user is responsible for inappropriate use or security violations which result. Choose and protect your passwords carefully. A good way to help secure your workstation temporarily is to set a screensaver password.

- You should always use your computer while logged into the Kentucky Department of Education networking environment, this will insure that your working files are scanned for viruses.
- If a starting password is used on a workstation, passwords must be given to district technology personnel.
- Downloading programs and installing personal software onto departmental computers and/or networking environment is strictly prohibited without written approval from the District Technology Coordinator. Bringing in software increases the risk of viruses.

Access to Electronic Media

(Staff Acceptable Use Policy)

MISUSE OF INFORMATION/TECHNOLOGY AND THE LAW

Kentucky statues identify criminal penalties for the following:

Criminal Damage to Property Law, Class D Felony KRS 512.010: a person is guilty of criminal mischief when, having no right to do so or any reasonable ground to believe that they have such a right, they intentionally or unintentionally deface, destroy, or damage any public agency date or technology property (date, computer programs, computer systems, computer networks, computers, etc.

Unlawful Access to a Computer, Class C Felony Kentucky Criminal Statue KRS 438.840-434.860: A felony may be committed when an individual goes beyond assigned duties to: knowingly and willingly, directly or indirectly, access, cause to be accessed, or attempt to access a computer system, data stored in a computer, or a network for the purpose of altering, damaging or destroying data or technology.

In simpler terms, these laws prohibit:

- Probing, which means using technology deliberately to gain access for which one is not authorized or to evade security procedures; and/or
- Vandalism, which means inappropriately altering or destroying data, damaging hardware, software, or network components. Vandalism also includes deliberate attempts to restrict or degrade the access of others to data and technology.

These laws do not prohibit systems administrators or other authorized personnel from examining files, transaction logs, or other information about an individual's use of technology if that examination is within the scope of the individual's assigned responsibilities. If an employee with such responsibilities misuses his/her authority or the information to which s/he has access, s/he is subject to disciplinary action or penalty.

If an employee is absent from work or unavailable, the employee's supervisor may be provided access to the employee's workstation, files, and email account without the employee's prior notice or permission.

EMPLOYEE USE

Employees may use electronic mail and other District technology resources, including but not limited to parent and student portal, 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. Staff members may not create personal social networking sites to which they invite students to be friends.

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.

Access to Electronic Media

EMPLOYEE USE (CONTINUED)

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 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.

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.

Use of School Property

Staff Acceptable Use of Electronic Information Resources Agreement

Staff Member's Name _____ Position _____

School _____

I have read the District Staff Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules, my account can be terminated, and I may face other disciplinary measures.

Staff Signature _____ Date _____

==========

This space reserved for System Administrator

Assigned Use Name: _____

Assigned Temporary Password: _____

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 005:120; 16 KAR 1:020 KAR 001:020 (Code of Ethics (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516

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

Adopted/Amended: 6/29/2015
Order #: 7838

Access to Electronic Media

EMPLOYEE USE (CONTINUED)

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 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.

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.

Use of School Property

Staff Acceptable Use of Electronic Information Resources Agreement

Staff Member's Name _____ Position _____

School _____

I have read the District Staff Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules, my account can be terminated, and I may face other disciplinary measures.

Staff Signature _____ Date _____

==========

This space reserved for System Administrator

Assigned Use Name: _____

Assigned Temporary Password: _____

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 005:120; 16 KAR 1:020 KAR 001:020 (Code of Ethics (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516

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

Adopted/Amended: 6/29/2015