Access to Electronic Media

(Acceptable Use Policy)

The Board supports the right of students, employees and community members to have reasonable access to various information formats and believes it is incumbent upon students, employees, and community members 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.

This policy outlines both the privileges and the responsibilities associated with the use of the Scott County Schools' network and its resources. It addresses ethical and educational uses of electronic media, including, but not limited to, the Internet, email, and other technological resources. It also addresses issues of privacy versus administrative review of electronic files and communications. The policy prohibits use of networks for illegal activities, the intentional spreading of embedded messages, or the use of other programs with the potential of damaging or destroying programs or data.

For additional information see school board policies for students, and certified and classified employees, regarding use of school property, disrupting the educational process, and conduct.

Educational Suitability

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.

Network Reliability

Scott County Schools will not be responsible for any damages not limited to loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its own negligence or user errors or omissions.

Safety

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 are reasonably believed to 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 Chief Information Officer to enable access by an adult employee for bona fide research or other lawful purpose.

Accounts are to be used in support of education and research that is consistent with the educational objectives of the Scott County Schools. This may include **reasonable** personal use. Examples of acceptable use include, but are not limited to, protecting yourself and others by not revealing personal information that could lead a stranger to you or another person. (i.e. name, address, telephone, workplace, etc.) Users should notify a Principal or School Technology Coordinator (STC) of any policy violations or security breaches. This can be done anonymously.

No employee, contractor, volunteer, or other adult working directly with students enrolled in the District shall engage in any sexually related behavior with a student utilizing electronic communications, including but not limited to sexual jokes; sexual remarks; sexual kidding or teasing; sexual innuendo; and pressure for dates or sexual favors. If an employee, contractor, volunteer, or other adult working directly with students enrolled in the District utilizes a student's telephone number, email address, or user/screen name on a messaging service or social networking site, which was obtained from school records, for a purpose inconsistent with this policy, such use constitutes a misuse of personally identifiable information or educational records and may result in discipline, up to possible termination of employment.

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.

Due to potential legal and ethical risks posed by interacting with students, staff members are strongly discouraged from creating personal social networking sites with which they interact with students. Employees taking such action do so at their own risk.

Unacceptable Use

Guidelines for unacceptable use 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. Unacceptable use of technology includes, but is not limited to, the following;

- Violating State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information;
- Sharing your password;
- Using or altering anyone else's password;
- Allowing someone to access any area of your account;
- Accessing any computer or network for which you are unauthorized;
- Creating or sharing computer viruses;
- Destroying another person's data;
- Monopolizing the network resources by running large programs and applications over the network during the day and/or sending massive amounts of email to other users, or using system resources for games;
- Vandalizing network resources;
  Vandalism is defined as any attempt to harm or destroy equipment, data, operating systems or applications, our network, or any other networks. It also includes "hacking" or gaining unauthorized access to computers or computer systems, or attempting to gain such unauthorized access.
- Playing games with no educational purpose over the network;
- Taking from or placing on the network, any copyrighted material including copyrighted movies and music without authorization from the District network administrator;
- Distributing or collecting obscene, abusive, discriminatory or threatening material via telephone, video, email, internet or other means;
- Demonstrating or discussing policy violations or security breaches with someone other than a school network administrator;
- Annoying other users with things such as talk requests and chain letters;
- Conducting any illegal activity via the network; Known illegal activity will be reported to the authorities;
- Sending harassing, intimidating, or abusive messages to others;
- Using vulgar, profane, obscene, or other inappropriate language;
- Using network resources for personal profit; and
- Using technology resources for commercial, political, or profit-making enterprise except as specifically agreed to with the District.
-

Access Privileges to Electronic Materials

Access to electronic information resources may range from read-only access to instructional software to full search capability of the Internet and to email. For these reasons the Scott County Schools maintain the right to limit access to software and/or documents found either on our network or the Internet via technical or human barriers.

Network Privileges

Employees	Students	Community Members
Infinite Campus or similarly necessary information systems, when appropriate	User folder	Internet access
User folder	Supervised internet access and supervised class email (P-3)	
Internet access	Independent internet access and independent email (4-12)	
Email account		

Contracts

Student

A contract, signed by the student, shall be required prior to the school granting that student access to the network, Internet and/or email. The signature of a parent or guardian is also required for students under the age of eighteen (18) and will indicate the degree of access granted to the student. This document shall be kept on file by the Principal or School Technology Coordinator (STC) as a legal, binding document and shall continue to be in effect throughout the student's attendance in the building in which their grade level is housed (i.e. Preschool, K-5, 6-8 and 9-12), unless modified by the parent/guardian. These signatures indicate understanding and agreement with the specified acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations.

Employee

A contract, signed by the employee, shall be required prior to the school granting that employee access to the network, Internet and/or email. This document shall be kept file by the Chief Information Officer as a legal, binding document. The signature indicates understanding and agreement with the specified acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations.

Community Member

The Chief Information Officer shall determine when it is appropriate for community members to have access to District technology resources.

A contract, signed by the community member, shall be required prior to the school granting that community member access to the network, Internet and/or e-mail. This document shall be kept on file by the Chief Information Officer, Principal or School Technology Coordinator (STC) as a legal, binding document.

The signature indicates understanding and agreement with the specified acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations.

Logins and Passwords

Upon signing a contract, a private login and password will be assigned to each user. The user is responsible for any activity performed under that login and password and therefore, passwords must be kept private.

There will be no access to the network, email, or the Internet without the use of a login and password and those will only exist for those persons with a signed contract.

Right to Privacy

The Scott County Schools reserve the right to ask the Chief Information Officer to access any user folder and/or email account of any user at any time. Users are advised not to place confidential documents in their user folder and never to use email for confidential communication. Email is not private.

All Internet sites visited will be logged and reviewed for suitability of Internet use to assure compliance with the AUP and with state law. Internet access has been granted for educational and research purposes only.

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 technological resources.

Responsibility for Damages

Individuals shall reimburse the Board for repair or replacement of District property lost, stolen, damaged, or vandalized while under their care.

Disciplinary Action

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.

Any user who violates the terms and conditions of this Acceptable Use policy will experience immediate degradation of services to "read only access". Loss of privileges may continue for a period of up to one (1) calendar year, and/or other disciplinary actions may be enforced as per the discipline policy.

The CIO or STC may convert an account to "read only access" at any time as required. The CIO or STC in cooperation with the building administrator, must notify the user, and user's parents in case of a minor, in writing within two weeks informing them of the reason for suspension or termination of an account.

Disciplinary Action (continued)

Users (student, employees, or community members) whose accounts are denied, suspended or revoked do have the following rights:

1. To request (in writing) from the Chief Information Officer a written statement justifying the disciplinary actions.
2. To submit a written appeal to the Superintendent and a committee he/she shall designate. Pending the decision of this committee, a user can make a final appeal to the Board of Education. The decision of the Board of Education is final.

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 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; 47 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516
15-ORD-190

Related Policies:

03.13214/03.23214
03.17/03.27
08.1353, 08.2322, 09.14; 09.4261
10.5

Adopted/Amended: 4/21/2016
Order #: 28

If you need the full size copy of the document, please follow the link below to view it in a larger font.

http://www.scott.kyschools.us/docs//building/20/aup2016fullsize.pdf

OR

If you have a QR Reader on your Smart Phone or Tablet, you can scan the code below to open the document.