CURRENT POLICY

CURRICULUM AND INSTRUCTION 08.2323

Access to Electronic Media

(Acceptable Use Policy)

The Board supports reasonable access to various information formats for students, employees and the community and believes it is incumbent upon users to utilize this privilege in an appropriate and responsible manner.

SAFETY PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for access to electronic media. Guidelines shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail, and other District technological resources), and issues of privacy versus administrative review of electronic files and communications. In addition, guidelines 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.

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.

Internet safety measures shall be implemented that effectively 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 minor's access to materials harmful to them.

The District shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate its Internet safety measures.

Specific expectations for appropriate Internet use shall be reflected in the District's code of acceptable behavior and discipline including appropriate orientation for staff and students.

PERMISSION/AGREEMENT FORM

A written parental request shall be required prior to the student being granted independent access to electronic media involving District technological resources.

The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges, and penalties for policy/procedural violations, must be signed by the parent or legal guardian of minor students (those under 18 years of age) and also by the student. This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Superintendent with a written request.

EMPLOYEE USE

Employees shall not use a code, access a file, or retrieve any stored communication unless they have been given authorization to do so. (Authorization is not required each time the electronic media is accessed in performance of one's duties.) Each employee is responsible for the security of his/her own password.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

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 District guidelines to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication, Live@edu 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 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 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.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

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.

COMMUNITY USE

On recommendation of the Superintendent/designee, the Board shall determine when and which computer equipment, software, and information access systems will be available to the community.

Upon request to the Principal/designee, community members may have access to the Internet and other electronic information sources and programs available through the District's technology system, provided they attend any required training and abide by the rules of usage established by the Superintendent/designee.

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.

RESPONDING TO CONCERNS

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.

AUDIT OF USE

Users with network access shall not utilize District resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system.

Access to Electronic Media

(Acceptable Use Policy)

AUDIT OF USE (CONTINUED)

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
2. Maintaining and securing a usage log; and
3. Monitoring online activities of minors.

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:

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

Access to Electronic Media

The Magoffin County School District offers access to telephones and the District computer network for Internet, E-mail, and video/digital pictures. To gain access to District technology, all students and staff must sign and return a user agreement form. Students who are under 18 years of age must have the form signed by a parental/guardian. Students who are eighteen years of age or older, may sign their own user agreement form. The signed user agreement form shall be returned to the school Principal and shall remain in effect and kept in the student's file for as long as s/he is enrolled in and attending a District school.

Access to District telephones, Internet, E-mail, and video/digital pictures will enable students/staff to explore thousands of libraries, databases, and bulletin boards and to exchange information with Internet users throughout the world. However, families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate and/or offensive. The District uses Proxy servers to filter Internet sites; however, filtering software is not 100% effective. Although filters make it more difficult to receive/access objectionable material, they are not a solution in themselves. While our intent is to make Internet access available to advance educational goals and objectives, students may find ways to access non education related materials/information. For this reason, we have an acceptable use policy to address access issues. We believe the benefits from access to the Internet and its information resources and opportunities for collaboration exceed any disadvantages. Ultimately, it is the parents/guardians of minors who are responsible for setting and conveying the standards that children should follow when using District technology. To that end, the District supports and respects each family's right to decide whether or not to apply for access.

GENERAL RESPONSIBILITY FOR DISTRICT TECHNOLOGY

Students and staff are expected to exhibit responsible behavior when using school computers, networks, the Internet, video/digital pictures and telephones. Since communications on the network are often public in nature, general school rules and policies apply. The District provides supervision by a certified teacher or other trained and designated adult to monitor students who are using District technology.

Access to District technology is a privilege, not a right and it requires users to be responsible for their behavior. Users are required to comply with District rules and regulations and to honor the agreements they have signed.

Every user will receive a password to log in to the computer and a folder on the server (H:Drive/Filelocker) where his/her work can be saved. Users will not lose what they are working on and their work will be saved until they leave the District or graduate.

Network administrators may review files and communications to maintain system integrity and to insure that users are using the system responsibly. Users should not expect that files stored on District servers will be private. Within reason, freedom of speech and access to information will be honored.

Access to Electronic Media

GENERAL RESPONSIBILITY FOR DISTRICT TECHNOLOGY (CONTINUED)

Some software packages allow the District's systems administrator to view, intervene in and "take over" a user's screen. These packages are designed to diagnose and troubleshoot network problems and to support help desk activities. Although they are not designed to scan network activity for inappropriate use, the District may use them for that purpose. In addition, through this software, school administrators can receive detailed information about each Internet access/ telephone use and individual users can be traced. These logs are stored for regular monitoring.

THE SCHOOL COUNCIL AND COMMUNITY: INFORMATION ABOUT THE VALUE OF THE NETWORK

The School Based Decision-Making Council, with District guidance and assistance, is an appropriate entity to provide parents and the community with accurate and timely information about how technology resources are being used to support student achievement. Parent and community education can be accomplished through the Student Technology Leadership Program (STLP), and by inviting parents to participate in classroom and parent/community workshops.

Parent/community education programs will help parents to understand, appreciate and support the use of technology in the schools, to make informed judgments about potential risks associated with the use of the Internet and to provide appropriate guidance for home use.

TELEPHONE AND OTHER VOICE SYSTEMS

The District has installed a Voice Over IP System in all schools. The school/classroom telephones are designed to aid, support and protect the instructional process. Phones are not to be used for personal, public, private or commercial purposes. No telephone calls from outside the school will go directly into the classroom.

Each school Principal will adopt and implement procedures for student use of voice (telephone) systems and how the school will address telephone calls or messages (Voice mail, secretary messages, etc.) to and from the classroom.

RIGHTS AND RESPONSIBILITIES

As outlined in Board Policy and Administrative Procedures and in the Student Handbook and Code of Conduct, students/staff do have Rights and Responsibilities. While rights and responsibilities will be adhered to, **the following will not be permitted** when using Magoffin County's Internet, E-mail, Video/Digital Pictures or Telephones/Cell Phones:

Electronic Media:

- Sending or displaying offensive messages or pictures through any type of electronic media;
- Swearing, vulgarities, or other inappropriate languages;
- Harassing, threatening, insulting or attacking others through electronic media;
- Sending electronic messages anonymously;

Access to Electronic Media

Electronic Media (continued):

- Sending or attaching documents containing pornographic, obscene, sexually explicit material or language;
- Accessing, copying or transmitting another's messages and/or attachments without permission; and/or
- Sending or forwarding any form of malicious code (e.g. chain letters, viruses, etc.).

Safety Cautions:

- Revealing personal student identification, either about himself/herself or any other user;
- Trespassing in another's folders, work, files or accessing another's email or network account;
- Attempting to login as a system administrator;
- Using the network to facilitate plagiarism. No user shall misrepresent another person's work as his/her own, or allow his/her work to be misrepresented as belonging to someone else;
- Viewing, entering, and participating in any chat room activity will not be permitted;
- Transmitting illegal, alcohol, or drug related information;
- Transmitting information or communicating with gangs, hate groups, or groups with violent themes; and/or
- 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 and etc.

Telephone:

- Sending/receiving messages or phone calls relating to or in support of illegal or harmful activities; and/or
- Use that interrupts instruction. Use must be limited to a minimal amount of time. (Daily logs are kept on file.)

Internet Usage:

- Using any type of email or instant messaging (Ex Hotmail, Yahoo, MSN, etc) other than that which is provided by the District;
- Using Non-Instructional GAMES on the network;
- Downloading non-instructional material from the Internet (i. e. music, games, videos);

Local Technology Resources:

- Employing the network, email or telephone for commercial or personal purposes;
- Violating copyright laws;
- Damaging computers, computer systems, computer networks, or school/District websites. This includes changing control panel settings and/or altering teacher preferred settings.

Access to Electronic Media

Local Technology Resources (CONTINUED):

- Intentionally infecting a computer or network with a virus program;
- Accessing Streaming Media that is non-educational or that is not of value to Instruction such as music videos and etc.;
- Monopolizing the networks by such things as running large programs and applications or sending massive amounts of mail to others;
- Allowing a non-authorized user to use one's account;
- Gambling, purchasing, or soliciting non-educational materials;
- Emailing communications that are not directly related to instruction, sanctioned school activities or a person's job;
- Using E-mail for private business or personal non-work related communications;
- Destroying another user's data
- Allowing another person to use one's E-mail or network account

AUDITING PROCEDURES

- Proxy server software shall be implemented and maintained at the District level and at every school on a twenty-four hour, seven day a week basis.
- Logs of Internet activity shall be examined periodically to detect access to sexually explicit or other objectionable material, as defined by the school's site based council and District technology committee.
- The school Principal/designee shall have the responsibility for log maintenance, examination, security and retention.
- Electronic mail shall be monitored periodically to ensure that users are not misusing school resources or using non-compliant email systems.
- Telephone logs shall be examined periodically to monitor proper usage.

Users are held accountable for the additional rules and regulations found in the Magoffin County Schools Electronic Access & Usage Plan. Violation of these rules and regulations may result in the suspension or revocation of a user account as well as other disciplinary or legal action.

VIOLATION PROTOCOL

- Fill out AUP Violation Form Letter.
- For student violations, send copy home to parents; email copy to lab teacher, librarian, homeroom teacher, and Principal. For staff member violations, send copy to staff member and Principal.
- Set reminder for time to reset account according to violation number.
- As appropriate, file signed copy of form letter in student's cumulative folder or employee's personnel file.

Staff Use of Telecommunication Devices

Employees issued a telecommunication device are responsible for its safekeeping at all times. Defective, lost or stolen equipment (pagers, digital or cell phones, etc.) are to be reported immediately to the Central Office so that the service provider may be notified.

Telecommunication devices issued to employees are to be returned to the Central Office designee at the conclusion of the school year, activity or as otherwise specified.

RESTRICTIONS

All drivers shall comply with applicable legal requirements concerning use of cellular telephones and other personal communication devices while operating a Board-owned vehicle.

- Employees shall not engage in activities that distract them from safely operating a vehicle.
- Except for communications made to and from a central dispatch, school transportation department, or its equivalent, drivers shall not use a telecommunication device, including those used for calling, texting or emailing while operating a Board-owned vehicle unless the vehicle is parked or unless there is a bona fide emergency, which shall include, but not be limited to the following actions:
    1. Report illegal activity;
    2. Summon medical help;
    3. Summon a law enforcement or public safety agency; or
    4. Prevent injury to a person or property.
- Telecommunication devices are not to be used for conversations involving District information of a confidential nature.
- Board-owned telecommunication devices are not to be loaned to others.

REIMBURSEMENT

1. On a monthly basis, the using employee shall highlight, on a copy of the telecommunication device billing, any emergency calls made/received.
2. Once personal calls have been highlighted, the employee shall calculate the cost of emergency personal usage and write a check for that amount to the District.
3. The employee shall submit the check to the Central Office, along with the highlighted copy of the billing statement, for review and recommendation for approval.

Review/Revised:7/19/11

Electronic Access/User Agreement Forms

USER CONTRACT - CLASSIFIED, CERTIFIED STAFF AND ALL OTHER USERS

Teachers and others whose duties include classroom management and/or student supervision should be knowledgeable about school safety/technology use issues including detecting, deterring, and documenting inappropriate use, safe-guarding personal privacy, and dealing with unsolicited online contact.

I have read the District's Acceptable Use Policy and related administrative procedures, and I agree to use the District's network and other technology in an acceptable, responsible and appropriate manner and to observe proper network etiquette. I understand that I am responsible for my own personal behavior when I am using the Internet, District network/programs, Video/Digital pictures, E-Mail and telephones. I agree that if I commit any violation, my access privileges may be revoked and school disciplinary action and /or appropriate legal action may be taken including the following:

1st offense – One week suspension from all electronic media and letter of notification to immediate supervisor

2nd offense – Two week suspension from all electronic media and letter of notification to immediate supervisor

3rd offense – Suspension from all electronic media for the remainder of the school year and a conference with my supervisor and the Superintendent

Note: All notifications and documentation of any offense will be kept on file in personnel folder.

Name (please print) _____

Signature _____

School _____

Date _____ School Year _____

Adults: Return this form to your TIS or Program Director