STUDENT ACCESS TO ELECTRONIC MEDIA

Electronic access including Internet, social networking tools, and e-mail shall be in support of education and research. Limited personal use of technology is permitted as long as the use does not interfere with the employee's job duties or performance and must comply with acceptable use guidelines.

PROCEDURES AND GUIDELINES FOR GAINING ACCESS TO DISTRICT RESOURCES

All District classrooms are wired and provided access to the District network. Staff members shall have user/e-mail accounts on the network upon signing the Acceptable Use Policy User Agreement. Staff members are responsible for all activities associated with their account and for the security of their password.. Staff members using the Infinite Campus Internet Portal shall follow all rules of acceptable use as specified in this policy.

All students may access the District network upon signing the Acceptable Use Policy User Agreement. The agreement must also be signed by the parent or guardian. Students (grades 6-12) shall have individual user/e-mail accounts on the network. Students in grades K-5 shall have user accounts, and they may have email accounts upon request from the Principal. Students are responsible for all activities associated with their account and for the security of their password. Students are not allowed to use network resources or Internet access without reasonable teacher or instructional assistant supervision. The Powell County School District manages student information electronically and students in grades 4-12 will be able to view their educational record via a secure connection over an Internet Portal. Students using the Infinite Campus Internet Portal shall follow all rules of acceptable use.

Consultants, legal counsel, independent contractors and other persons having business with the District may be granted user privileges for educational purposes at the discretion of the Superintendent or designee.

Except in cases involving students who are at least eighteen (18) years of age and have no legal guardian, parents/guardians may request that the school/District:

- Provide access so that the parent may examine the contents of their child(ren)'s email files;
- Terminate their child(ren)'s individual email account and/or Internet access; and
- Provide alternative activities for their child(ren) that do not require Internet access.

Any staff member or student who wishes to use personally owned mobile devices on the District network, property owned or leased by the Board, or during school-sponsored trips and activities, shall adhere to all guidelines in the District Acceptable Use Policy and accompanying procedure(s).

Additional guidelines for the use of personally owned devices are:

- Use of the device during school hours will be for educational purposes and at the discretion of the individual schools and classroom instructor.
- Students and staff shall only use the District wireless network (not private data cellular service) during school hours.

ACCESS TO ELECTRONIC MEDIA

PROCEDURES AND GUIDELINES (CONTINUED)

- A maximum of three (3) devices may be registered at the same time to students. The device must have wireless capability and should sustain battery power for a minimum of two (2) hours.
- Students shall not use devices to take and/or distribute photos or videos except for educational purposes and with the permission of a teacher.
- Powell County Schools will not be held responsible for any physical damage, loss or theft of the device. A student or staff member who brings their personally owned device to school is responsible for the device as well as all security, maintenance, and repair. Electrical access will not be provided for charging these devices while on school property.

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.

INTERNET SAFETY

The Powell County School District takes annual measures to ensure that staff and students are safe from potential threats while using the resources of the internet for teaching and learning. These annual measures are:

- A public hearing or meeting to address and communicate District Internet safety measures.
- Staff training on the Acceptable Use Policy and accompanying procedure(s) which includes parental consent, teacher supervision, and auditing procedures.
- Managing and monitoring the proxy server as required in KRS 156.675.
- Updating/reviewing the list of allowed blocked websites on the proxy server.
- Educating staff about The Children's Internet Protection Act (CIPA), The Children's Online Privacy Protection Act (COPPA), The Protection of Pupil Rights Amendment (PPRA), The Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPPA).
- Safety Instruction to all Students – Schools shall complete the Powell County Schools Internet Safety/Digital Citizenship Form. This form shall document the age appropriate instruction provided by the schools with regard to Internet Safety, appropriate responsible behavior while online, on social networking sites, and in chat rooms, and cyber bullying awareness and response. All original documentation shall be kept at the school and a copy submitted to the Powell County District Technology Coordinator.

ACCESS TO ELECTRONIC MEDIA

INTERNET SAFETY (CONTINUED)

The District network, electronic resources provided by the District, and the District website may be used for the purpose of supplementing classroom instruction with social networking tools to promote communications with students and parents concerning school-related activities. District employees shall comply with the following procedure:

- Attend District training before receiving account rights/permissions to the District website.
- Set up the site following District guidelines as specified in the training.
- The District Technology Coordinator/designee shall retain access to the site after granting account permissions/rights to staff members.
- Monitoring, managing, updating the site regularly, and observing confidentiality restrictions concerning release of student information under state and federal law.
- No external personal webpages may be linked from the District website.

Staff may use online educational services under the following conditions:

- Staff shall not utilize online educational services which require social security or driver's license numbers from minors without permission from the Principal and express written permission from the parent/guardian.
- Any online service must be for educational purposes and comply with local, state and federal laws.
- Prior to the purchase of an online educational service or software, administrators must receive approval from the District Technology Coordinator.
- Prior the use of an online education service or software, staff must receive approval from their supervisor.
- Photos of students and school events may be posted to the school website, without personally identifiable information, upon written consent from the parent/guardian.

NO PRIVACY GUARANTEE

A network administrator, the DTC or designee has the right to access information in any user directory, on the current user screen or in electronic mail. Users are advised not to place confidential or objectionable documents in their user directory. The DTC/designee monitors Internet usage via the Proxy servers and in accordance with SB230. The Proxy logs are maintained for a minimum of sixty (60) days. The DTC/designee may periodically examine Internet activity to detect access to sexually explicit or other objectionable material. The Coordinator shall also periodically monitor electronic MAIL to ensure that staff or students are using KETS approved mail systems. The Coordinator/designee may also monitor drives and storage devices (flash and jump drives, CDs, etc) connected to and used on district resources/computers.

ACCESS TO ELECTRONIC MEDIA

COPYRIGHTED MATERIALS

The use of copyrighted material for educational purposes, by school personnel, shall be within the generally accepted uses delineated by applicable law. All employees shall use electronic materials only in accordance with the license agreement under which the electronic materials were purchased or otherwise procured. Electronic materials are defined as computer software, databases, videotapes, compact and laser disks, electronic textbooks or any other copyrighted material distributed in electronic form. Any duplication of copyrighted electronic materials, except for backup and archival purposes, is a violation of the law, unless the license agreement explicitly grants duplication rights. The archival copy is not to be used on a second computer at the same time the original is in use. In addition, illegal copies of copyrighted software shall not be used on District equipment. The Superintendent/designee shall sign all District software license agreements. The DTC shall have on file a copy of all executed software licenses or original documentation of software purchased by the District. Employees shall have on file a copy of all executed software licenses, the original disk or the original documentation of software purchased for their individual workstations. Employees shall not install any software on individual workstations without permission from the DTC.

NETWORK, E-MAIL AND INTERNET REGULATIONS

The use of network and/or Internet accounts must be in support of education and research and be consistent with the educational objectives of the District. Staff members shall reasonably supervise student use of network resources (including, but not limited to, web based interactive tools). Parents/Legal guardians should accept responsibility for guiding their child in the appropriate use of Internet/e-mail.

Only KETS approved e-mail may be utilized on the District network. All District users shall access District resources by logging on and logging off each time they use a computer.

As a user of this network you may not:

- violate any US or state legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
- share your password or acquire/use someone else's password.
- Access, send, or post objectionable or threatening material, offensive messages or pictures including those that involve profanity or obscenity.
- alter network accounts or break in to the school's network, or attempt to bypass security measures to gain access to restricted programs.
- access a chat room on the Internet without authorization from the school.
- create or share computer viruses.

ACCESS TO ELECTRONIC MEDIA

NETWORK, E-MAIL AND INTERNET REGULATIONS (CONTINUED)

- destroy another person's files or trespass in another person's folders, work or files.
- Use or connect to District resources any storage devices (flash drives, floppies, CDs, external hard drives, etc.) containing inappropriate or objectionable material.
- monopolize the resources of the network by such things as running large programs and applications, sending massive amounts of mail, accessing unauthorized chat rooms or playing games (unless considered educational by your teacher).
- violate any copyright laws or plagiarize (including software copyright laws and digital works).
- damage computers, computer systems, computer networks, or school/District websites.
- use the network for illegal activities, private business, profit, political lobbying, or religious statements.
- use offensive language, threaten or harass, or intimidate others.
- reveal any personal information such as your name, address or telephone number without permission from the teacher or parent/guardian.
- create or forward chain letters.
- use any other e-mail account other than KETS-approved standards.
- bypass the proxy server or access any website/program that bypasses the proxy server.
- use 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 or Xanga.com.

Note: Your e-mail account should not be considered private. The DTC shall periodically scan e-mail accounts for objectionable materials and non-compliance.

Additional rules and regulations concerning use of District technology are available on request from the District Technology Coordinator.

RELATED PROCEDURE:

08.2321 AP.1; 08.2323 AP.21

Review/Revised:6/9/14