Henderson County Schools
1805 Second Street, Henderson, Kentucky 42420
(270) 831-5000 Fax: (270) 831-5009
http://www.hendersonschools.net

DATE: June 12, 2012

TO: Dr. Thomas L. Richey, Superintendent
And Henderson County School Board Members

FROM: Marganna Stanley, Assistant Superintendent of Administration

RE: Digital Devices

The purpose of this memo is to update you on the progress of the use of personal digital devices on our network. Linda Payne has secured a program that will allow employees and students to obtain a Digital Drivers License (DDL). A DDL will be required from any employee or student before their personal electronic device may be used on our network.

The hardware process (wiring, access points, switches) will be completed by the middle of July 2012 at Central Office, the Technology Support Building, and South Middle School per Mike Bruner.

Conversations have begun with Mr. Ryan Reusch and Mrs. Becky Johnson for safe implementation of the use of personal devices. Policy and procedures have been reviewed and revised.

Formatted: Centered

Telecommunication Devices

TELECOMMUNICATIONS DEVICES DEFINED

Telecommunications devices are defined to include, but are not limited to, paging and portable music devices, cellular phones, cameras, and other similar electronic devices used to deliver communications.

POSSESSION AND USE

1. Devices shall not be used in a manner that disrupts the educational process, including, but not limited to, use that:
   a. Poses a threat to academic integrity, such as cheating,
   b. Violates confidentiality or privacy rights of another individual,
   c. Is profane, indecent, or obscene,
   d. Constitutes or promotes illegal activity or activity in violation of school rules, or
   e. Constitutes or promotes sending, sharing, or possessing sexually explicit messages, photographs, or images using any electronic device.

   These restrictions shall not be interpreted to prohibit material protected under the state or federal constitutions where such material does not otherwise materially or substantially disrupt the education process or intrude upon the rights of others.

Students are responsible for keeping up with devices they bring to school. The District shall not be responsible for loss, theft, or destruction of devices brought onto school property.

Students shall comply with any additional rules developed by the school concerning appropriate use of telecommunication or other electronic devices.

Students shall not utilize a telecommunication or similar electronic device in a manner that would violate the District's Acceptable Use policy or procedures or its Code of Acceptable Behavior and Discipline.

ELEMENTARY AND MIDDLE SCHOOL

A student in the Henderson County Schools, grades P-8, shall not use/display a telecommunications device while on school property during the regular school day unless authorized by a certified employee.

HIGH SCHOOL

A student in grades 9-12 may use telecommunication devices during non-instructional times as defined by school policy.

Unless an emergency situation exists that involves imminent physical danger or a certified employee authorizes the student to do otherwise, devices shall ~~be~~remain turned ~~on~~off and operated only before and after the regular school day and during the student's lunch break.

Formatted: ksba normal

When students violate prohibitions of this policy, they shall be subject to disciplinary action, including losing the privilege of bringing the device onto school property and being reported to their parent/guardian. A violation also may result in a report being made to law enforcement. In addition, an administrator may confiscate the device, which shall only be returned to the student's parent/guardian.

Telecommunication Devices

CONSEQUENCES

First Offense: In-house or out-of-school suspension and the parent may pick up the telecommunication device the next school day.

Second Offense: In-house or out-of-school suspension and the parent may pick up the telecommunication device the next school day.

Subsequent Offense: Severe disciplinary action, including, but not limited to, out-of-school suspension, short term placement or long term placement at Central Learning Center (CLC) and the parent may pick up the telecommunication device the next school day.

Note: Telecommunication devices confiscated on a Friday may be picked up on Monday by a parent or guardian. Parents or guardians will need to contact the Principal to make arrangements if the telecommunication device is confiscated before holidays or breaks.

NOTICE OF POLICY

Notice of this policy and penalties for violating it shall be published annually in the District's Code of Conduct handbook.

REFERENCE:

[1]KRS 158.165

RELATED POLICIES:

08.2323
09.426
09.436
09.438

LEGAL: BOARDS RECEIVING E-RATE FUNDING FOR INTERNET ACCESS ARE REQUIRED TO UPDATE THEIR INTERNET POLICY CONCERNING DISABLING OF PROTECTION MEASURES. ADDITIONAL CHANGES ARE SUGGESTED TO MEET OTHER REQUIREMENTS OF FEDERAL LAW (CHILDREN'S INTERNET PROTECTION ACT).
FINANCIAL IMPLICATIONS: NONE ANTICIPATED

DRAFT 6/13/12

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 as required by this policy and related procedures, which apply to all parties who use District technology.

Formatted: ksba normal

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, 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 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;
- Education of minors about appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Formatted: Bullets and Numbering

- 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 that are deemed obscene, child pornography, or harmful to ~~them.~~minors.

A technology protection measure may be disabled by the Board's designee during use by an adult to enable access for bona fide research or other lawful purpose.

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

Access to Electronic Media

(Acceptable Use Policy)

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 use electronic mail, technology resources, and network access only for purposes directly associated with work-related activities.

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.

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.

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.

District employees and activity sponsors may not set up social networking accounts using District resources or create such accounts associated with a school/District location or organization unless specific authorization is given by the Superintendent/designee.

District employees and activity sponsors may set up authorized blogs 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.

In order for District employees and activity sponsors to utilize a District approved blog or authorized social networking account 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, an authorized site will be established by the Superintendent's designee and specific permissions will be set for the appropriate school personnel to conduct and monitor blogging activities.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

a. Once the blog site or authorized social networking account has been created, and permissions set, the sponsoring staff member is responsible for the following:

b. Monitoring and managing the site(s) to promote safe and acceptable use; and

c. 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 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.

Access to Electronic Media

(Acceptable Use Policy)

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.

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.

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least five (5) years after the last day of service in a particular funding year.

Formatted: ksba normal

Formatted: policytext

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.~~47 U.S.C. 254/Children's Internet Protection Act; 45 C.F.R. 54.520
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

EXPLANATION: THESE CHANGES ARE RECOMMENDED TO CLARIFY THE TYPES OF ACCEPTABLE USE OF TECHNOLOGY VIOLATIONS THAT WILL SUBJECT THE USER TO POSSIBLE CONSEQUENCES. FINANCIAL IMPLICATIONS: NONE ANTICIPATED

DRAFT 6/13/12

Formatted: Centered

Access to Electronic Media

The District offers access to and use of technology, the Internet and email as part of the instructional process.

Students must sign a Student Acceptable Use Policy agreement before direct access to technology, the Internet or teacher directed electronic mail (email) would be provided. Written parental consent shall be required before any student is given direct, hands-on access to technology, the Internet or to teacher-directed electronic mail. However, educators may use the Internet during class-directed group demonstrations with or without parental consent. Students will be held accountable for violations of the Student Acceptable Use Policy agreement and understand that disciplinary action may be taken.

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.

Parents/guardians wishing to challenge information accessed via the District's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

Local Technology Resources

- Users shall not violate State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.

Formatted: Indent: Left: -0.05", Hanging: 0.3", Tab stops: 0.25", List tab + Not at 0.2"

Formatted: Bullets and Numbering

- The use of your account, District devices, and network resources must be in support of education and research consistent with the District's educational objectives.
- Any use of the computer network must conform to state and federal law, network provider policies and licenses, and District policy.
- Use of the computer network for charitable purposes must be approved in advance by the Superintendent/designee.
- The computers and computer network constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
- Users may not give their passwords to anyone.
- Users may not transmit, access, or store obscene, profane, abusive threatening, or sexually explicit language.
- Users may not create or share computer viruses, worms, or other malicious code.
- Users may not destroy another person's data.
- Users may not damage or destroy any technology or related devices, such as computer systems, computer networks, or school/teacher/District websites.
- Users may not use the network for commercial purposes.

Access to Electronic Media

LOCAL TECHNOLOGY RESOURCES (CONTINUED)

- Users may not monopolize the resources of the District's network by such things as running large programs and applications over the network during the day, sending massive amounts of email to other users, or using system resources for nonacademic games or gaming.
- Users may not break or attempt to break into other computer networks.
- Users are responsible for the appropriateness and content of material they store, transmit, or publish on the network. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
- Users may not participate in MUD (multi-use games) via the network.
- Users are not permitted to get from, or put into, the network copyrighted material (including software), or threatening or sexually explicit material. Copyrights must be respected.
- ~~Personal devices may only be brought to school by staff members with specific permission of the building administrator. No District network access will be granted for these devices.~~
- Staff members may bring personal devices for work-related use at school/work locations with specific permission of the building administrator/designee.
- Students may bring personal devices for educational use at school only after receiving a digital driver's license and specific permission of the building administrator/designee.
- Personal devices, both staff and students, will only be permitted to join the District network after each user has successfully completed a digital citizenship course and received a digital driver's license.
- Student personal devices may only be used in the classroom with permission of the teacher.
- Staff members who wish to loan their personal devices to students should do so with caution, for instructional purposes only, and only when accessing the network and Internet via District resources.

Formatted: Not Highlight
Formatted: Bullets and Numbering
Formatted: Not Highlight
Formatted: Not Highlight
Formatted: Not Highlight

INTERNET REGULATIONS

- Network and Internet access through the school is to be used for instruction, research, and school-related activities. School access is not to be used for private business or personal, nonschool-related communications.
- Teachers, Library Media Specialists, and other educators are expected to select instructional materials and recommend research sources in print or electronic media. Educators will select and guide students on the use of instructional materials on the Internet.
- Users may not offer network or Internet access to another individual via their District accounts.
- Student users may not offer use of their personal devices to other student users.
- Purposefully annoying other Internet users, on or off the District system, is prohibited. This includes such things as continuous talk requests, unauthorized social networking contacts, and chat rooms.
- Students shall not reveal their own names or personal information to or establish relationships with "strangers" on the Internet, unless a parent or teacher has coordinated the communication.

Formatted: Not Highlight
Formatted: Indent: Hanging: 0.25"
Formatted: Bullets and Numbering

Access to Electronic Media

INTERNET REGULATIONS (CONTINUED)

- Students shall not reveal the names or personal information of other students.
- Technology resources shall not be used to bully, threaten or attack a staff member or student.
- Technology resources shall not be used to access and/or set up unauthorized blogs and online journals, including, but not limited to such sites as MySpace.com, Facebook.com or Xanga.com.
- The school and school personnel shall never reveal a student's personal identity or post a picture of a student or a student's work on the Internet with personally identifiable information unless the parent has given written consent.
- School personnel must acquire specific permission to create student accounts on websites, programs, or technology services that are not hosted on District servers.
- Students shall notify their teacher(s) or another adult whenever they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable.
- Network accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their passwords with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their accounts.
- Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.
- Communications may not be encrypted so as to avoid security review.
- A student who does not have a signed AUP on file may not share access with another student.

Users of this educational system should notify a network administrator or a teacher of any violations of this contract by other users or outside parties. This may be done anonymously.

The District reserves the right to remove a user account on the system to prevent further unauthorized activity.

ELECTRONIC MAIL REGULATIONS

- Students and employees of the District are prohibited from using District resources to establish Internet E-mail accounts through third party providers. Only Kentucky Education Technology Systems E-mail may be used.
- Users are expected to be polite. No user is allowed to write or send abusive messages to others.
- Users may only send electronic mail for communications that are directly related to instruction or sanctioned school activities. They shall not use electronic mail for private business or personal, non-work or non-school related communications.
- Users may not swear, use vulgarities or any other inappropriate language.
- Users may not send or attach documents containing pornographic, obscene, threatening, or sexually explicit material.

Access to Electronic Media

ELECTRONIC MAIL REGULATIONS (CONTINUED)

- Users may not access, copy or transmit another user's messages without permission.
- Users should not reveal a personal address or phone number or those of other students unless a parent or a teacher has coordinated the communication.
- Users may not send electronic messages using another person's name or account.
- Users may not send electronic messages anonymously.
- Users may not create, send, or participate in chain E-mail.

Users should not expect files stored on District servers or through District provided or sponsored technology services, to be private. People who operate the system do have access to all mail Messages relating to or in support of illegal activities may be reported to the authorities.

KNOWLEDGE, INFORMATION AND DATA SERVICES TO REFLECT EXPANDED STUDENT ACCESS TO ONLINE TECHNOLOGIES.
FINANCIAL IMPLICATIONS: NONE ANTICIPATED

DRAFT 6/13/12

CURRICULUM AND INSTRUCTION 08.2323 AP.21

Student User Agreement and Parent Permission Form

DIRECTIONS: After reading the Student Acceptable Use Policy and related administrative procedures for District technology, Internet and E-mail access, please read and fill out the appropriate portions of this contract completely and legibly. The signature of a parent or guardian shall be required for direct access for all students. Please return the contract to your child's teacher.

I have read the Student Acceptable Use Policy and related administrative procedures for technology, Internet and E-mail access. I understand and will abide by the stated Terms and Conditions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. If I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

Student Name (please print) _____

Student Signature: _____ Date _____

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the District's Student Acceptable Use Policy and related procedures for technology, Internet and E-MAIL access. I understand that this access is designed for education purposes and that District schools have taken available precautions to eliminate access to controversial material. However, I also recognize it is impossible for District employees to restrict access to all controversial materials, and I will not hold District personnel responsible for materials this student may acquire on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission for the student named above to have Internet access and certify that the information contained on the form is correct.

CONSENT FOR USE ~~OF LIVE@EDU~~

~~The Outlook Live e-mail solution is provided to your child by the District as part of the Live@edu service from Microsoft.~~ By signing this form, you hereby accept and agree that your child's rights to use the ~~Outlook Live e-mail service~~electronic resources provided by the District~~,~~ and/or ~~other Live@edu services as~~ the Kentucky Department of Education (KDE) ~~may provide over time,~~ are subject to the terms and conditions set forth in District policy/procedure ~~as provided.~~ Please also be advised ~~and~~ that ~~the~~ data stored in relation to such ~~Live@edu~~ services~~, including the Outlook Live e-mail service,~~ is managed by the District pursuant to policy 08.2323 and accompanying procedures. You also understand that the ~~Windows Live ID~~ e-mail address provided to your child can also be used to access other electronic services or technologies that may or may not be sponsored by the District, which ~~that~~ provide features such as online storage, online communications and collaborations, and instant messaging. Use of those ~~Microsoft~~ services is subject to either ~~Microsoft's~~ standard consumer terms of use ~~(the Windows Live Service Agreement), or a standard consent model. and data stored in those systems is managed pursuant to the Windows Live Service Agreement and the Microsoft Online Privacy Statement.~~ 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 your child can use online ~~those Microsoft~~ services, he/she must accept the ~~Windows Live~~ service agreement and, in certain cases, obtain your consent.

Parent or Guardian (please print) _____

Parent's/Guardian's Signature: _____ Date _____

~~**OPTIONAL**~~

~~**AUTHORIZATION TO POST STUDENT'S PICTURE/PHOTO**~~

~~I give permission for this student's picture to appear on District/school web sites.~~

~~Parent's/Guardian's Signature: _____ Date _____~~

~~**AUTHORIZATION TO POST STUDENT WORK**~~

~~I give permission to display the product of this student's school-related academic, athletic, musical and/or art work on the District/school web sites.~~

~~Parent's/Guardian's Signature: _____ Date _____~~

Formatted: Centered

Formatted: Font: 10 pt, Not Highlight

Formatted: Font: 10 pt