2016-2017 STAFF ACCEPTABLE USE POLICY

CURRICULUM AND INSTRUCTION 08.2323

Access to Electronic Media and Industrial Technologies

INTRODUCTION

The Laurel County School System (LCSS) provides staff and students a telecommunication network and other new technologies in order to carry out the educational business of LCSS in conducting and accessing research, and in communicating with others in regard to instructional or job related functions.

KRS 156.675 requires that each school district adopt and implement an acceptable use policy. The purposes of the policy are to educate, to provide protection against violations of privacy, to prevent misuse of public resources, to protect against inappropriate or destructive behaviors, and to ensure that technology resources are dedicated to improving student achievement and school administration.

The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students and model the appropriate use of such resources.

The LCSS electronic communications system has a purpose limited to educational usage**.** This policy will govern all use of the LCSS Electronic Communication Network. 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. Student use of the system will also be governed by school disciplinary codes.

Students and staff are responsible for legal, ethical, and appropriate behavior on school computer networks just as they are in a classroom or school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. The network is provided for students to conduct research and to communicate with others for instructional enhancement. Only students who submit signed permission and agreement forms by parents and students will be permitted network access. Permission forms must be submitted on a yearly basis. Only staff who submit signed acknowledgment and agreement forms will be permitted network access and use of district technology. This signature sheet 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) or the staff member must provide the Superintendent/designee with a written request. 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 of other computing and telecommunications technologies.

INTERNET

The LCSS makes every attempt to keep our students and staff safe while on the Internet. Internet access is monitored through a proxy server; and software is in place to filter unacceptable or offensive sites. Although we make every effort to block inappropriate material, families should be aware that users may unexpectedly come across sites that contain sites with offensive or inappropriate material. If that happens, they should report this to the proper officials immediately. Users who are found deliberately searching for this type of material and or repeatedly visiting those sites will have their Internet privilege revoked. All users must

authenticate to the LCSS network and will be assigned a designated user-id login and password. This login to the Domain will authenticate each user that logs into the Laurel County Domain.

Access to Electronic Media and Industrial Technologies

SOCIAL NETWORKING

The Kentucky School Board Association and the Laurel County School District discourage staff from creating personal social networking sites i.e., MySpace, Facebook, Twitter, etc., wherein they accept or invite students to be friends or allow them access to their social networking site. Employees taking such actions do so at their own risk. Staff who utilize social networking sites should be mindful of privacy settings that would prevent students or the public in general from accessing their personal information such as status updates and photo galleries.

EMPLOYEE USE

All employees shall be subject to disciplinary action if their conduct relating to use of technology violates this or other applicable policy or statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel r requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. This code also extends to public online behavior including social networking. Conduct in violation of this code must be reported to the Educational Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action, up to and including termination of employment.

ELECTRONIC MESSAGING

LCSS realizes that personal email is an acceptable form of communication but use of this type of communication should be limited. Employees shall use electronic media in a professional manner consistent with state laws governing the behavior of school employees and with federal laws governing copyright infringement. Staff will employ electronic email on a daily basis at work as a basic tool for communications. Staff will be responsible for checking and reading messages daily. Electronic mail and telecommunications are not to be utilized by employees to share confidential information about students or other employees except for administrative purposes only. In discussing students or confidential information, staff should be aware that email generated or stored by the LCSS is subject to Open Records. Network and school administrators may review files and communications to maintain system integrity and to ensure that staff members and students are using the system responsibly.

The LCSS-provided email system is the only email system that is to be used on the LCSS System network.

If the connection feature in the system provided by the District and/or the Kentucky Department of Education (KDE) is utilized to connect with private accounts i.e., gmail, Hotmail, or Yahoo mail, or any other account not affiliated with the systems provided, the private email account becomes a .org owned account, meaning it is owned by the LCSS, and therefore is subject to all Board policies as well as this policy.

The email system provided by the District and/or the Kentucky Department of Education (KDE) includes Instant Messaging capabilities. However, it is the position of the LCSS that this function not be utilized in the Laurel County School District. Use of the Instant Messaging is a direct violation of this policy and will result in disciplinary action and or loss of network privileges.

Access to Electronic Media and Industrial Technologies

TELEPHONES

Telephones are a part of the telecommunications network and are considered as part of the system resources. The same procedures and regulations therefore apply that govern other electronic media.

PRIVACY

Users of the LCSS network should be aware that information accessed, created, sent, received, or stored on the network is not private and is subject to be reviewed by network and school administrators. The District reserves the right to access and monitor all messages and files on the LCSS network.

PROHIBITED BEHAVIORS

The following behaviors are NOT permitted on the District network or machines:

Staff and Students

- Hotmail and other email clients and accounts shall not be accessed from the Laurel County network. If accessed via connection capabilities provided by the District and/or the Kentucky Department of Education (KDE), those accounts become owned by the LCSS and are privy to all Board policies.
- Sending or displaying offensive messages or pictures (this includes profanity, nudity, pornography, vulgarity, racism)or harassing or insulting messages. Depending on the nature or content, disciplinary action may be taken, and these may also be reported to law enforcement.
- Engaging in practices that threaten the network (i.e., loading files that may introduce a virus, or file sharing software such as Swaptor, Direct Connect WinMX Napster, eDonkey 2000, Filetopia, etc.). The preceding list is by no means exhaustive or complete.
- Violating copyright laws.
- Trespassing in others folders, documents, or files or using others' passwords.
- Intentionally wasting limited resources.
- Using the network for commercial purposes, i.e., advertising a product or selling a product to make money such as a jewelry party, Avon orders, Mary Kay parties, food parties, i.e., anything that generates income for an individual is prohibited. The purchasing of goods for personal use is also prohibited.
- Promoting or campaigning for individuals or political parties or soliciting contributions to a political campaign, party or issue.
- Shall not violate any Federal or State regulations.
- Purposely bypassing the proxy server.
- General audio and visual streaming/ download/rip any music to store on computers network .
- Stream music or radio.
- Accessing sites to online chat rooms or software that enables online posting and receiving of real-time messages i.e., Yahoo Instant Messenger, etc. Although the email client has instant messaging capabilities, instant messaging is PROHIBITED by the LCSS and its AUP.
- Sending electronic messages anonymously.
- Sending electronic messages using another person's name or account.
- Accessing/playing MUD (multi-user games) via the network or any non-educational computer game whether online CD, flash drive, etc.

Access to Electronic Media and Industrial Technologies

PROHIBITED BEHAVIORS (CONTINUED)

- Sending mass emails (districtwide emails) for non school related purposes.
- Accessing online communities such as MySpace, Facebook, etc.
- Access gambling sites.
- Cyberbullying.

Staff Personal Mobile Devices

- Staff personal mobile devices, such as, but not limited to, cell phones, iPads, tablets, iPods, or other personally owned mobile devices, may be utilized to access the Internet and email accounts for instructional purposes once that device is registered with the LCSS wireless network via the staff members domain login account. Registration with the LCSS wireless network insures device compliance with proxy filtering and internet protection solutions. Use of personal data plans on personally owned devices during the instructional day is strictly forbidden and a direct violation of this policy, State law, and the Child Internet Protection Act.
- Staff PDAs, Blackberries, or laptops that are brought into the LCSS with a WLAN card may be used during the school day to access the Internet for instructional purposes once that device is registered with the LCSS wireless network via the staff member's domain login account.. Only computers accessing the LCCS network shall be used for accessing the Internet.
- Student personal electronic devices, such as, but not limited to, cell phones, iPads, Tablets, iPods, or other personally owned electronic devices, are not to be utilized to access the Internet, personal email accounts, social networking sites such as MySpace, Facebook, or Twitter, or Instant Messaging, during the school day. Doing so is a direct violation of this policy, State law, and the Child Internet Protection Act.
- PDAs, Blackberries, or laptops that are brought into the LCSS with a LAN card shall not be used during the school day to access the Internet. Only computers accessing the LCCS network shall be used for accessing the Internet.
- Staff is responsible for their assigned laptops when taking them home. District owned laptops are for professional use and should be treated as such. Staff members' laptops shall not be used as a home computer for other family members; staff shall keep in mind that student records are contained within the District owned laptop.
- Telephone/cell phone usage shall be planned to occur during the planning period when staff are not responsible for students.
- When taking students into a lab setting or allowing students on computers in a classroom, staff shall always provide adequate supervision.

DISREGARD OF RULES

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

Students or staff who deface District property shall be subject to disciplinary action, up to and including expulsion or termination, as appropriate.

Access to Electronic Media and Industrial Technologies

INDUSTRIAL TECHNOLOGIES

PURPOSE

The Board supports reasonable access to various technology 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.

That Board recognizes that the industrial technology field employs creative and technically proficient individuals who can help a company achieve efficient and profitable productivity. Industrial technology is the use of engineering and manufacturing technology to make production faster, simpler and more efficient.

Industrial technology skills are now fundamental for students who want a future in engineering and technology. The Board expects that staff will equip these students with such information and training and that the staff will provide guidance and instruction to students in the appropriate use of such technology.

The purpose of the District's industrial technology program is limited to educational usage to assist in preparing students for success in the 21st century.

RESTRICTIONS AND REQUIREMENTS

Users may not utilize the industrial technologies for commercial purposes, defined as the direct or indirect use of any part of an industrial technology, in any form, for sale, resale, solicitation, rent or lease of a service, or any use by which the user expects a profit either through commission, salary or fee or service for personal use unless authorized by the Board.

This policy will govern all use of industrial technologies. Student use of the system also will be governed by the District and school disciplinary codes.

Students are responsible for good behavior when using industrial technology. The following behaviors are not permitted when using District industrial technologies:

1. The creation of weapons, parts of weapons, or lethal objects of any sort, or any device that resembles the same for the purpose of creating the impression that the object created is a weapon, part of a weapon, or lethal object, whether for personal use or demonstration.
2. The creation of any objects containing profanity or obscenity.
3. The creation of any objects that could be construed as drug paraphernalia, parts of drug paraphernalia, or any device that resembles the same for the purpose of creating the impression that the object is drug paraphernalia or part of drug paraphernalia.
4. The creation of any objects that could be construed as inappropriate body parts.

Employees are encouraged to use industrial technology to promote student learning. If those resources are used, they shall be used for purposes directly related to work-related activities.

Technology-based materials, activities and tools shall be appropriate for, and with the range of, the knowledge, understanding, age and maturity of students with whom they are used.

Students shall be provided instruction about appropriate and safe behavior when using industrial technology including, but not limited to, the use of safety equipment.

Access to Electronic Media and Industrial Technologies

CYBERBULLYING

It is the policy of the Laurel County Board of Education that all students and school employees enjoy a safe and secure educational setting. The school prohibits cyberbullying, as defined herein. Nothing in this policy is intended to infringe on the constitutional rights of students or school employees.

DEFINITIONS

The term "cyberbullying" means the use of any electronic communication, by individuals or groups, to:

a. make a true threat against a student or school employee;

b. materially disrupt school operations; or

c. substantially impinge on the rights of another student such as, but not limited to: creating reasonable fear of harm to the student's person or property; creating a substantially detrimental effect on the student's physical or mental health; substantially interfering with a student's academic performance or interfering with the student's ability to participate in or benefit from the services, activities, or privileges provided by the school; or being so severe, persistent, or pervasive as to cause severe emotional distress.

Cyberbullying includes conduct that is based on, but not limited to, a student's actual or perceived race, color, national origin, gender, religion, disability, sexual orientation or gender identity, distinguishing physical or personal characteristic, socioeconomic status, or association with any person as identified above.

As used in this policy, the term "electronic communications" means communications through any electronic device, including, but not limited to, computers, telephones, mobile phones, pagers, and any type of communication, including, but not limited to, emails, instant messages, text messages, picture messages, and websites.

SCHOOL JURISDICTION

No student shall be subjected to cyberbullying by an electronic communication that bears the imprimatur of the school regardless of whether such electronic communication originated on or off the school's campus.

The school shall have jurisdiction to prohibit cyberbullying that originates on the school's campus if the electronic communication was made using the school's technological resources or the electronic communication was made on the school's campus using the student's own personal technological resources.

The school shall have jurisdiction to prohibit cyberbullying that originates off the school's campus if:

1. it was reasonably foreseeable that the electronic communication would reach the school's campus; or

2. there is a sufficient nexus between the electronic communication and the school which includes, but is not limited to, speech that is directed at a school-specific audience, or the speech was brought onto or accessed on the school campus, even if it was not the student in question who did so.

Access to Electronic Media and Industrial Technologies

CYBERBULLYING

NOTICE

a. Parents shall receive written notice of this cyberbullying policy at the beginning of each school year.

b. There shall be an annual process for discussing this policy with students in a student assembly.

c. For access to the school's technological resources, including but not limited to email and Internet access, students and parents shall review, sign, and return the school's acceptable use policy which prohibits the use of the school's technological resources for Cyberbullying

d. This policy, along with the school's acceptable use policy shall be prominently posted at school on student bulletin boards and in computer labs, and on the school's website as well as the Student Code of Conduct.

INVESTIGATIONS

Parents shall be notified as soon as practicable if their child is involved in a school investigation concerning cyberbullying.

School officials may search and seize a student's personal electronic device, including but not limited to cell phones and computers, if:

1. the student is using the electronic device at school in violation of school rules; or
2. the school official has reasonable grounds for suspecting the search will turn up evidence that the student has violated or is violating either the law or the school rules; and
3. the search is limited in scope by being reasonably related to the objective of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.

Reasonable grounds, as set forth in item 2 above will not be established solely on anonymous reports.

If the cyberbullying victim or student reporting the cyberbullying is willing, the school shall initiate an interview to determine the nature of the bullying, the name of the participants, where and how the information was being sent, and how far the images or messages have spread.

Any evidence of cyberbullying discovered during an investigation should be preserved. Such actions may include, but are not limited to, saving the victim's cell phone, text, or email messages; and printing or copying posts or other electronic communications available on websites before removing them.

If, during the course of a cyberbullying investigation, images of nude minors are discovered, those images should not be distributed or shown to other school officials. The school official who discovered the image should promptly contact law enforcement.

Access to Electronic Media and Industrial Technologies

CYBERBULLYING

REPORTING

Specific faculty members [to be named by the schools] will be the main contacts for students who wish to report incidents of cyberbullying. Students, parents, and other school officials may also contact the principal to report incidents of cyberbullying.

Anonymous and confidential reports of cyberbullying incidents are allowed, but they will not provide the sole basis for a search of a student's personal electronic device or for disciplinary action.

School officials may report incidents of cyberbullying to law enforcement depending on the criminal nature of the offense, or the gravity and repetition of the offense.

REMEDIES

An individual student whose behavior is found to be in violation of this policy will be subject to discipline. In determining the disciplinary action, the school will take into consideration the nature of the offense, the age of the student, and the following:

a. For a first-time or minor cyberbullying offense, the school may mandate that the student attend mandatory counseling and education sessions.

b. For a second or more serious cyberbullying offense, the school may prohibit the student from participating in school activities or events.

c. For a serious incident of cyberbullying, the school may suspend or expel the student.

No student shall retaliate or make false accusations against a target or witness of cyberbullying.

Wherever practicable, the school shall provide counseling to all students involved in a cyberbullying incident.

Whenever practicable, the school shall file a complaint with Internet sites or services containing cyberbullying material to have the material removed.

EDUCATION

The school shall provide an annual educational program for students, parents, and school officials. This education program shall train individuals:

1. on the meaning of and prohibition against cyberbullying, including the provisions of this policy;
2. how students can report cyberbullying incidents
3. how students can be an ally to peers who are being cyber bullied; and
4. how students can protect themselves from being cyber bullied.

The school shall encourage students to play an active role in developing the school's cyberbullying educational programs.

Access to Electronic Media and Industrial Technologies

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)

RELATED POLICIES:

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

Adopted/Amended: 7/8/2013
Order #: Section IV,#1

PERSONNEL 03.13214

- CERTIFIED PERSONNEL -

Use of Personal Cell Phones/Telecommunication Devices

Due to privacy concerns, and except for emergency situations, personally owned recording devices are not to be used to create video or audio recordings or to take pictures while on duty or working with students except with prior permission from the Principal/designee or immediate supervisor.

An exception may be made for events considered to be in the public arena (e.g. sporting events, academic competitions, or performances to which the general public is admitted) where the activity does not materially disrupt the event, prevent others from observing the event, or otherwise violate legal rights. School social events for students, activities sponsored by student clubs, and activities during the school day that are not open to the public are not considered to be in the public arena.

Such devices include, but are not limited to, personal cell phones and tablets.

Adopted/Amended: 7/27/2015
Order #: 3.1