

2017-2018 STUDENT ACCEPTABLE USE POLICY TO ACCESS ELECTRONIC MEDIA

Introduction:

The Laurel County School System (LCSS) provides 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 and limited to educational usage.

Kentucky Senate Bill 230 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. Specific expectations for appropriate Internet use shall be reflected in the District's code of acceptable behavior and discipline including appropriate orientation for students. Student use of the system will also be governed by school disciplinary codes. Students 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. 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. 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/designee with a written request. This signature sheet shall be kept on file as a legal, binding document. 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 Telecommunication technologies.

Cell Phone:

While cell phones may be appropriate for use during extracurricular activities, they are NOT appropriate for use during the school day. Ringing phones, text messaging and phone photography are disruptive to the instructional environment. While on school property during the instructional day (8:15 a.m. –3:05 p.m.), students shall be permitted to possess personal communication devices/electronic devices given the following guidelines:

1. Devices may only be used before and after the instructional day.
2. Students are responsible for keeping up with devices they bring to school. A school's faculty and staff are not responsible for loss, theft, or destruction of devices brought onto school property.
3. Students shall not utilize a telecommunication or similar electronic device in a manner that would violate the district's Acceptable Use Policy or school SBDM Policy.

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

Internet:

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

Electronic Messaging:

Students shall use electronic media in a professional manner consistent with the Student Code of Conduct and with federal laws governing copyrights. Students 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 students are using the system responsibly. LCSS realizes that personal email is an acceptable form of communication but this type of communication should be limited. The LCSS provided email system is the only email system that is to be used on the LCSS System network. The Office 365 e-mail provided to you by the district is a part of the Office 365 service from Microsoft. By signing this form, you accept and agree that your rights to use the Office 365 service, and other Office 365 services as the Kentucky Department of Education may provide, over a period of time, are subject to the terms and conditions set forth in district policy/procedure as provided and that the data stored, including Office 365 email, are managed by the district. You also understand that the Office 365 can be used to access other electronic services that provide features such as online storage and instant messaging. Use of those Microsoft services is subject to Microsoft's standard consumer terms of use and are managed pursuant to the Office 365 Agreement and Microsoft Online Privacy Statement. Before you can use those Microsoft services, you must accept the Office 365 Service Agreement. If the Connection feature in Office 365 system is utilized to connect with private accounts i.e. ...gmail, hotmail, or yahoo mail, or any other account not affiliated with Office 365, the private email account becomes .org owned account, meaning it is owned by the LCSS, and therefore is subject to all LCBOE policies as well as the LCSS AUP.

The Office 365 email system 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 the LCSS AUP and will result in disciplinary action and or loss of network privileges.

Privacy:

Users of the LCSS network should be aware that information accessed, created, sent, received, or stored on the network, including but not limited to Microsoft Email, G-Suite shares and OneDrive for business, 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.

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

- Hotmail and other e-mail clients and accounts shall not be accessed from the Laurel County network. If accessed via the Office 365 connection capabilities, those accounts become owned by the LCSS and are privy to all LCBOE policies and the LCBOE AUP.
- 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, 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, etc... Anything that generates income for an individual or for profit business is prohibited. The purchasing of goods for personal use is also prohibited.
- Promoting or campaigning for individuals, political parties and/or issues, 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. Although the Office 365 . . . LIVE@edu 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...
- sending mass emails (districtwide emails) for non-school related purposes
- accessing online communities such as MySpace, Facebook, Twitter, or Instagram, etc...
- access gambling sites
- cyberbullying is bullying

Personal Mobile Devices:

- 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 the LCSS AUP, KY SB 230, and the Child Internet Protection Act.
- PDAs, Blackberries, or Laptops that are brought into the LCSS with a LAN/WLAN card shall not be used during the school day to access the Internet. Only district provided computers and mobile devices connected to the LCCS network shall be used for accessing the Internet.

DISREGARD OF RULES:

Students shall be subject to disciplinary action up to and including but not limited to, having computer use and/or Internet privilege revoked and expulsion for violating this policy and acceptable use rules and regulations established by the school or District.

REFERENCES:

KRS 156.675; 701 KAR 005:120 16 KAR 1:020 KAR 001:020 (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

INDUSTRIAL TECHNOLOGIES AND CYBERBULLYING

Industrial Technologies Purpose:

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. 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.

The Board supports reasonable access to various technology formats.

Users should utilize this privilege in a responsible manner as required by this policy and related procedures, which apply to all parties who use District technology.

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.

Restrictions and Requirements:

Users may not utilize industrial technologies for commercial purposes. The use of any part of an industrial technology, in any form, to create items or services by which the user expects a profit either through commission, salary or fee for service, for personal use, is strictly prohibited unless authorized by the Board.

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.

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 substantially infringe 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.

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.

- 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 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.

REPORTING:

Students who wish to report incidents of cyberbullying should contact any school faculty member. 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. The discipline action range is conference to expulsion.

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

EDUCATION:

The school shall provide annual cyberbullying educational information to students.

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

REFERENCES:

KRS 156.675; 701 KAR 5:120 16 KAR 1:020 (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;