Access to Electronic Media Terms and Conditions 2020-2021

The Board of Education supports the right of students and employees to have reasonable access to various technology resources, including Internet and email, and believes it is incumbent upon students and employees to use this privilege in an appropriate and responsible manner.

ACCEPTABLE USE: Use shall be restricted to work-related tasks and educational objectives. To ensure appropriate use of resources and network security, the following procedures must be followed:

- Users may not violate State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
- Users may not share network accounts or passwords with anyone or gain unauthorized access to computers or computer systems, or attempting to gain such unauthorized access.
- Users shall not violate copyright laws, including illegal copying of commercial software and/or other protected material.
- Users may not access or alter another user's account.
- Users may not attempt to or break into other networks or secure locations on the schools' or District's networks, or in any way jeopardize the security of school or District networks, including attempts to bypass the District internet filtering and security solutions.
- Users may not damage computer systems, computer networks or school/District websites.
- Users may not create or share computer viruses.
- Users may not use District resources for games, chatting, or visiting inappropriate sites to access inappropriate material/information such as, but not limited to, pornography, hacking, gambling, gaming, unauthorized email, social networking, and gossip sites.
- Users may not utilize 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 social networking sites, such as but not limited to MySpace.com, Facebook.com or Xanga.com.
- Users may not use District resources to access e-mail accounts other than those established by the District for their use.
- Users may not destroy equipment or another user's data.
- Users may not monopolize system resources by sending massive amounts of mail, running large programs during school hours, using streaming music or video other than for authorized educational purposes.
- Students may not download programs of any type. District employees may download approved work-related programs.
- Users shall not use power-on passwords, screen saver passwords or screen savers.
- Users shall not use computers, including laptops, for personal use.
- Users shall not use the network for commercial purposes, financial gain or any illegal activity.

ETHICAL USE: Transmission of any material in violation of any U.S., state or local regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Use for product advertisement or political purposes is not permissible. 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.

NO PRIVACY GUARANTEE: The Superintendent/designee has the right to access information stored in any user directory, on the current user screen, or in electronic mail. Users are advised NOT to place confidential information or documents in these locations. Net management and monitoring software may be used for random access to student and staff accounts to monitor appropriate use of resources. Users should not expect files stored on District servers or through District provided or sponsored technology services, to be private. A network management system tracks all Internet and email activity. This system records sites visited, length of visits, the user name and the email content. Logs of Internet traffic and email activity will be reviewed periodically to ensure that sites and email communications are appropriate and offer educational value.

CONSEQUENCES: Any person responsible for the intentional destruction of equipment will reimburse the school system for the cost of replacing equipment. Intentional destruction or theft of equipment, software, or data will be punished to the full extent of school policies and state and federal legislation. For elementary school students, any violation of the AUP will result in immediate revocation of access to electronic resources for a minimum of nine (9) weeks. A second offense will result in permanent revocation of access. Any user whose access has been revoked may be recommended for alternative education. Additional consequences are at the discretion of the building Principal. For high school students, any violation of the AUP will result in timely disciplinary action including but not limited to student conference, parent conference, computer re-imaging, detention, in-school suspension, confiscation of the computer and/or restricted access, placement in alternative education, suspension, expulsion, financial restitution (in accordance with the board-approved fee schedule) and/or appropriate legal action. These and additional consequences specified in Site-Based Decision Making policy shall be administered or recommended by the Principal/designee.

AUTHORIZATION: As a user, I have read and fully understand the requirements and consequences in this permission statement. I understand that access is provided for educational purposes and that the District has taken available precautions to eliminate access to inappropriate material. However, I realize that it is impossible for the District to restrict access to all controversial material, and I assume responsibility for my own actions.

_____ _____

Student's Legal Name (Please print) ***Student's Signature***

_____ Chose one _____

Date ***Grade*** ***School Attending***

As the parent or legal guardian of the student signing above, I grant permission for my child to access networked computer services such as electronic mail and the Internet. I understand that this access is designed for educational purposes; however, I also recognize that some materials on the Internet may be objectionable, and I accept responsibility for guidance of Internet use by setting and conveying standards for my child to follow when selecting, sharing, researching, or exploring electronic information and media.

PARENT CONSENT FOR USE: By signing this form, you hereby accept and agree that your child's rights to use the electronic resources provided by the District and/or the Kentucky Department of Education (KDE) are subject to the terms and conditions set forth in District policy/procedure. Please also be advised that data stored in relation to such services is managed by the District pursuant to policy 08.2323 and accompanying procedures. You also understand that the 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 provide features such as online storage, online communications and collaborations, and instant messaging. Use of those services is subject to either standard consumer terms of use or a standard consent model. 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 services, he/she must accept the service agreement and, in certain cases, obtain your consent.

_____ _____ _____

Name of Parent/Guardian/Employee (Please print) ***Signature of Parent/Guardian/Employee*** ***Date***

*Employee (Location & Position)*_____ *Pass Phrase (15 Characters)*_____