APPROPRIATE USE OF DISTRICT TECHNOLOGY, NETWORK SYSTEMS, AND INTERNET ACCESS

The Board of Directors of the Riceville Community School District is committed to making available to students and staff members access to a wide range of electronic learning facilities, technology (including, but not limited to, computers, tablets, and hand held devices), equipment, software, network systems, and internet access. The goal in providing this technology and access is to support the educational objectives and mission of the Riceville Community School District and to promote resource sharing, innovation, problem solving, and communication. The District's technology, network, and/or internet access is not a public access service or a public forum. The District has the right to place reasonable restrictions on the material accessed and/or posted through the use of its technology, network, and/or internet access, including the use of personal technology brought into the District by students and staff and the ability of students and staff to access the District's network systems and internet access using personal technology.

The District's technology, network systems, and internet access shall be available to all students and staff within the District. However, access is a privilege, not a right. Each student and staff member must have a signed acceptable use agreement on file prior to using the District's technology, network systems, and internet access. The amount of time and type of access available for each student and staff member may be limited by the District's technology and the demands for the use of the District's technology. Even if students have not been given access to and/or use of the District's technology, network systems, and the internet, they may still be exposed to information from the District's technology, network systems, and/or the internet in guided curricular activities at the discretion of their teachers.

Every item of technology in the District having access shall not be operated unless internet access from technology is subject to a technology protection measure (i.e. filtering software). The technology protection measure employed by the District shall be designed and operated with the intent to ensure that students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are otherwise harmful to minors. The technology protection measure may only be disabled for an adult's use if such use is for bona fide research or other lawful purposes.

Administrators, faculty, and staff may request the technology coordinator to deny, revoke or suspend user accounts. Any user identified as a security risk or having a history of problems with appropriate use may be denied access to the District's technology, the District's network systems, and the District's internet access. Students and staff members will be instructed, at a minimum, on an annual basis by the District's technology coordinator or other appropriate personnel on the appropriate use of the District's technology, network systems, and internet access.

The use of the District's technology, network systems, and internet access shall be for educational purposes only. Students and staff members shall only engage in appropriate, ethical, and legal utilization of the District's technology, network systems, and internet access. Student and staff members' use of the District's technology, network systems, and internet access shall also comply with all District policies and regulations. The following rules provide guidance to students and staff for the appropriate use of the District's technology, network systems, and internet access. Inappropriate use and/or access will result in the restriction and/or termination of the privilege of access to and use of the District's technology, network systems, and internet access and may result in further discipline for staff members up to and including termination of employment and/or other legal action. The District's administration will determine what constitutes inappropriate use and their decision will be final. Inappropriate use includes, but is not limited to:

- Making or dissemination offensive or harassing statements or using offensive or harassing language including disparagement of others based on age, color, creed, national origin, race, religion, marital status, sex, sexual orientation, gender identity, physical attributes, physical or mental ability or disability, ancestry, political party preference, political belief, socioeconomic status or familial status.
- Swearing or using vulgarities or any other inappropriate language.
- Failing to be polite and/or not following the same privacy, ethical, educational, and other considerations observed regarding other forms of communication.
- Accessing, creating or disseminating any material that is obscene, libelous, indecent, vulgar, profane or lewd; any material regarding products or services that are inappropriate for minors including products or services that the possession and/or use of by minors is prohibited by law; any material that constitutes insulting or fighting words, the very expression of which injuries or harasses others; and/or any material that presents a clear and present likelihood that, either because of its content or the manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities, will cause the commission of unlawful acts or will cause the violation of lawful school regulations.
- Disseminating or soliciting sexually oriented messages or images.
- Transmitting personal credit card information or other personal identification information, including home addresses or telephone numbers from any District item of technology.
- Publishing personal or private information about yourself or others on the internet without prior written permission.
- Reposting a message that was sent to you privately without permission of the person who sent the message. Any information regarding students should be limited to the student's first name and the initial of the student's last name only.
- Arranging or agreeing to meet with someone met online.

- Using the District's technology, network systems, and/or internet access to participate in illegal activities, including but not limited to, gambling, fraud, and pornography.
- Subscribing to or accessing listservs, bulletin boards, online services, e-mail services, social networking sites (i.e. Facebook, Twitter) or other similar services without prior permission from the technology coordinator or other appropriate personnel.
- Using, possessing or attempting to make or dispute illegal/unauthorized copies of software or other digital media that has been downloaded or copied or is otherwise in the user's possession or is being used without the appropriate registration and/or license for the software or in violation of any applicable trademarks and/or copyrights, including the payment of any fees to the owner of the software or other digital media.
- Altering, modifying, corrupting or harming in any way the software stored on the District's technology or network systems, including installing any software on the District technology or on the District's network systems or running any personal software from either floppy disk, CD-ROM, DVD, flash drives or other storage media or altering or modifying any data files stored on the District's technology or network systems without prior permission and supervision from the technology coordinator or other appropriate personnel.
- Downloading programs or files from the internet without prior permission from the District's technology coordinator or other appropriate personnel. Any programs or files downloaded from the internet shall be strictly limited only to those that the technology coordinator or other appropriate personnel have approved for download.
- Using encryption software from any access point within the District.
- Accessing the internet from District technology using non-District internet or social networking account.
- Sharing personal user account information with anyone or leaving your account open or unattended.
- Accessing the District's technology or network systems or the District's internet connection from a non-District owned technology without prior authorization from the technology coordinator or other appropriate personnel.
- Disabling, circumventing or attempting to disable or circumvent filtering software.
- Playing games or running programs that are not related to the District's educational program.
- Vandalizing the District's technology or its network systems, including, but not limited to, any attempt to harm, modify, deface or destroy physical equipment or the network and any attempt to harm or destroy data stored on the District's technology or network or the data of another user. All users are expected to immediately report any problems or vandalism of technology equipment to the administration, the technology coordinator or the instructor responsible for the equipment.

- Committing or attempting to commit any act that disrupts the operation of the District's technology or network systems or any network connected to the internet, including, but not limited to, the use or attempted use or possession of viruses or worms or participation in hacking or other unlawful/inappropriate activities on line. Users must report any security breaches or system misuse to the administration or technology coordinator.
- Demonstrating any security or other network problems to other users; giving passwords to other users for any reason; and/or using another individual's account.
- Attempting to log on to any device as a system administrator.
- Using the network in such a way to cause a disruption in the use of the network by other users or wasting system resources (e.g. listening to internet radio, printing web pages without prior permission from the technology coordinator other appropriate personnel, staying on the network longer than is necessary to obtain needed information).
- Using the District's technology, network systems, and/or internet access for any commercial or for-profit purposes, personal or private business, (including but not limited to shopping, or job searching), product advertisement or political lobbying.
- Using the District's technology, network systems, and/or internet access, to download, transmit, and/or disseminate any material in violation of any federal or state law, copyrighted material, obscene material, hate literature, material protected by trade secret, viruses and/or worms, offensive material, spam emails, any threating or harassing materials, and/or material that will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities. If a user encounters potentially inappropriate information, the user shall immediately terminate contact with such information and notify the technology coordinator or other appropriate personnel of the contact with inappropriate information.
- Plagiarizing information accesses through the District's technology, network systems, and/or the internet. Students and staff shall obtain permission from appropriate parties prior to using copyrighted material that is accessed through the District's technology, network systems, and/or the internet.

Although reasonable efforts will be made to make sure students will be under supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students may encounter information that may not be of educational value and/or may be inappropriate. If a student encounters such information, the student should terminate access to the information immediately and notify supervisory personnel or other appropriate personnel of what occurred.

Students will be able to access the District's technology and network systems, including use of the internet, through their teachers and/or other appropriate supervisors. Students will not be allowed to use e-mail under very specific, limited educational circumstances. If a student has an

electronic mail address that has been set up outside of school, the student will not be permitted to access that e-mail account or use that address to send and receive mail at school.

Parents will be required to sign a permission form to allow their students to access the District's technology, network systems, and the internet. Students and staff members will sign a form acknowledging they have read and understand the District's policies and regulations regarding appropriate use of the District's technology and network systems, that they will comply with the policies and regulations, and understand the consequences for violation of the policy or regulations.

Prior to publishing any student work and/or pictures on the internet, the District will obtain written permission from the student's parents to do so.

The District has the right, but not the duty, to monitor any and all aspects of its technology, network systems, and internet access including, but not limited to, monitoring sites students and staff visit on the internet and receiving e-mails. The administration and the technology coordinator shall have both the authority and right to examine all technology and internet activities including any logs, data, e-mail, storage and/or other technology related records of any user. The use of e-mail is limited to District and educational purposes only. Students and staff waive any right to privacy in anything they create, store, send, disseminate or receive on the District's technology and network systems, including the internet.

No warranties, expressed or implied, are made by the District for the technology and internet access being provided. Although the District has taken measures in implement and maintain protection against the presence of viruses, spyware, and malware on the District's technology, network systems, and internet access, the District cannot and does not warranty o represent that the District's technology, network systems or internet access will be secure and free of viruses, spyware or malware at all times. The District, including its officers and employees, will not be responsible for any damages including, but not limited to, the loss of data, delays, non-deliveries, misdeliveries or service interruptions caused by negligence or omission. Individual users are solely responsible for making backup copies of their data. The District is not responsible for the accuracy of information users access on the internet and is not responsible for any unauthorized charges students or staff members may incur as a result of their use of the District's technology, network systems, and/or internet access. Any risk and/or damages resulting from information obtained from the District's technology, network systems, and/or internet access is assumed by and is the responsibility of the user.

Students, parents, and staff members may be asked from time to time to sign a new consent and/or acceptable use agreement to reflect changes and/or developments in the law or technology. When students, parents, and staff members are presented with new consent and/or acceptable use agreements to sign, these agreements must be signed for students and/or staff to continue to have access to and use of the District's technology, network systems, and the internet.

The interpretation, application, and modification of this policy are within the sole discretion of the Riceville Community School District. Any questions or issues regarding this policy should be directed to the superintendent, any building principal or the technology coordinator. The board of directors will review and update this policy as necessary.