Policy Title: **Appropriate Use of District Technology, Network Systems and Internet Access** Policy #605.1

The board 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 and software, network systems, and the internet. The goal in providing this technology and access is to support the educational objectives and mission of the school district and to promote resource sharing, innovation, problem solving, and communication. The district's technology, network and/or internet connection 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 connection, 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 having access to and using the district's technology, network and the internet.

Every item of technology in the district having internet access shall not be operated unless internet access from the item of 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.

The Director of Technology may close a user account at any time and the Director of Technology may deny, revoke or suspend user accounts at the request of the administration. Any user identified as a security risk or having a history of problems with technology and/or network systems may be denied access to the district's technology, network systems and the internet. Students and staff members will be instructed by the Director of Technology, or other appropriate personnel, on the appropriate use of the district's technology, network and the internet.

The use of the district's technology, network 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 member use of the district's technology, network and internet access shall 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 and internet access. Inappropriate use and/or access will result in the restriction and/or termination of the privilege of access to the district's technology, network and internet access. Inappropriate use by students may result in further discipline up to and including

expulsion. Inappropriate use by a staff member may result in further discipline 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 of the district's technology, network and internet access includes, but is not limited to a violation of the following rules:

- Do not make or disseminate offensive or harassing statements or use 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.
- Do not swear, use vulgarities or any other inappropriate language. Be polite and follow the same privacy, ethical, educational, and other considerations observed regarding other forms of communication.
- Do not access, create or disseminate 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. ~~a~~
- Any material that constitutes insulting or fighting words, the very expression of which injures 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 is prohibited.
- Do not disseminate or solicit sexually oriented messages or images.
- Do not transmit your credit card information or other personal identification information, including your home address or telephone number from any district item of technology without prior permission from the building principal, the superintendent or other appropriate personnel.
- Do not publish personal or private information about yourself or others on the internet without prior written permission.
- Do not repost a message that was sent to you privately without permission of the person who sent the message. If any information is to be provided regarding students, it should be limited to the student's first name and the initial of the student's last name only.
- Do not arrange or agree to meet with someone met online.
- Do not use the district's technology and/or network systems to participate in illegal activities and/or activities that are inappropriate for the workplace, including, but not limited to, gambling, fraud, and pornography.
- Do not subscribe to or access listservs, bulletin boards, online services, e-mail services, social networking sites (i.e., facebook, twitter, snap chat, etc.) or other similar services without prior permission from the Director of Technology or other appropriate personnel.
- Do not use, possess or attempt to make or distribute illegal/unauthorized copies of software or other digital media. Illegal/unauthorized software or other digital media means any software or other digital media that has been downloaded or copied or is otherwise in the user's possession or 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.

- Do not alter, modify, corrupt or harm in any way the software stored on the district's technology or network systems. Do not install any software on the hard drive of any district technology or on the district's network systems or run any personal software from either, CD-ROM, DVD, flash drives or other storage media or alter or modify any data files stored on the district's technology or network systems without prior permission and/or supervision from the Director of Technology or other appropriate personnel.
- Do not download any programs or files from the internet without prior permission from the district's Director of Technology or other appropriate personnel. Any programs or files downloaded from the internet shall be strictly limited only to those that you have received permission from the Director of Technology or other appropriate personnel to download.
- Do not use any encryption software from any access point within the district.
- Do not access the internet from a district item of technology using a non-district internet account.
- Do not share personal user account information with anyone.
- Do not access the district's item of technology or network systems or use the district's internet connection from a non-district item of technology without prior authorization from the Director of Technology or other appropriate personnel.
- Do not use an instant messenger service or program, internet relay chat or other forms of direct electronic communication or enter a chat room while using the district's technology, network systems and/or internet connection.
- Do not disable or circumvent or attempt to disable or circumvent filtering software without prior permission from the Director of Technology or other appropriate personnel.
- Do not play any games or run any programs that are not related to the district's educational program.
- Do not vandalize the district's technology or its network systems. "Vandalism" is defined as any attempt to harm, modify, deface or destroy physical technology or the network and any attempt to harm or destroy data stored on the district's technology or the 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.
- Do not commit or attempt to commit any act that disrupts the operation of the district's technology or network systems or any network connected to the internet, including 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 Director of Technology.
- Do not give your password to another user for any reason; and/or use another individual's account.
- Do not attempt to access any device as a system administrator.
- Do not use the district's technology and/or network systems 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.
- Do not use the district's technology, network systems and/or the internet to access,

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 e-mails, any threatening or harassing materials, and/or any 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.

- Do not plagiarize information accessed 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.

The district will, within the curriculum currently being offered, include age-appropriate content related to children's use of the internet. This may include anti-bullying and harassment considerations, social networking considerations and other considerations involving internet usage.

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 a non-school e-mail except 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, network systems and the internet; 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 permission via eRegistration from the student's parents.

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 reviewing e-mail. The administration and the Director of Technology shall have both the authority and right to examine all technology and internet activity 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 to 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 or 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, mis-deliveries 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 school district. Any questions or issues regarding this policy should be directed to the Superintendent, any building principal or the Director of Technology.

The board will review and update this policy as necessary. The district will maintain this policy at least five (5) years after the termination of funding pursuant to the Children's Internet Protection Act (CIPA) or E-rate.

Approved: 6/24/02

Reviewed: 12/22/08

Revised: 6/25/12; 2/24/14; 7/23/18