APPROPRIATE USE OF COMPUTERS, COMPUTER NETWORK SYSTEMS, AND THE INTERNET

The Board of Directors of the Clinton Community School District is committed to making available to students and staff members access to a wide range of electronic learning facilities, equipment, and software, including computers, computer network systems, and the internet. The goal in providing this technology and access is to support the educational objectives and mission of the Clinton Community School District and to promote resource sharing, innovation, problem solving, and communication. The District's computers, computer 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 computers, computer network, and/or internet connection.

Access to the District's computers, computer network systems, and the internet 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 computers, computer network systems, and the internet. 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 computers, computer network systems, and the internet, they may still be exposed to information from the District's computers, computer network systems, and/or the internet in guided curricular activities at the discretion of their teachers.

The school district will monitor the online activities of students and will educate students about appropriate online behavior, including interacting on social networking sites and chat rooms. Students will also be educated on cyber-bullying, including awareness and response. Employees will provide age appropriate training for students who use the Internet. The training provided will be designed to promote the school district's commitment to:

- The standards and acceptable use of Internet services as set forth in the Internet Safety Policy;
- Student safety with regard to:
  - safety on the Internet;
  - appropriate behavior while on online, on social networking Web sites, and
  - in chat rooms; and
  - cyber-bullying awareness and response.
- Compliance with the E-rate requirements of the Children's Internet Protection Act

Legal References: Iowa Code § 279.8 (2014).
Children's Internet Protection Act (2001)

Cross References:
502 Student Rights and Responsibilities
506 Student Records
605.5 Media Centers
605.9 Technology Protection Measures

Approved 3/11/1996 Reviewed 6/10/2019 Revised 4/14/2014

The use of the District's computers, computer 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 computers, computer network systems, and internet access. Student and staff member use of the District's computers, computer 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 computers, computer 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 computers, computer network systems, and internet access and may result in further discipline for students up to and including expulsion and/or other legal action 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 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; 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.

-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 computer. 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 computers and/or computer network systems to participate in illegal activities. Illegal activities include, but are 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. xanga, myspace, facebook) or other similar services without prior permission from the technology coordinator 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 computer software stored on the District's computers or computer network systems. Do not install any software on the hard drive of any District computer or on the District's computer network systems or run any personal software from either floppy disk, USB storage device, CD-ROM, DVD or other storage media or alter or modify any data files stored on the District's computers or computer network systems without prior permission and supervision from the technology coordinator or other appropriate personnel.

-Do not download any 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 you have received permission from the technology coordinator 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 computer using a non-District internet account.

-Do not share a personal user account with anyone. Do not share any personal user account passwords with anyone or leave your account open or unattended.

-Do not access the District's computers or computer network systems or use the District's internet connection from a non-District computer without prior authorization from the technology coordinator 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 computers, computer network systems, and/or the District' internet connection.

-Do not disable or circumvent or attempt to disable or circumvent filtering software.

-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 computers or its computer network systems. Vandalism is defined as any attempt to harm, modify, deface or destroy physical computer equipment or the computer network and any attempt to harm or destroy data stored on the District's computer equipment or the computer

network or the data of another user. All users are expected to immediately report any problems or vandalism of computer 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 computers or computer network systems or any network connected to the internet, including the use or attempted use or possession of computer 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. Do not demonstrate any security or other network problems to other users; give your password to another user for any reason; and/or use another individual's account. Do not attempt to log on to any device as a system administrator.

-Do not use the network in such a way that you would disrupt the use of the network by other users or would waste system resources (e.g. listening to internet radio, printing web pages without prior permission from the technology coordinator or other appropriate personnel, staying on the network longer than is necessary to obtain needed information).

-Do not use the District's computers and/or computer 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 computers, computer 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, computer 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 computer, computer 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 computer, computer 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 computers and computer network systems, including use of the internet, through their teachers and/or other appropriate supervisors. Individual electronic mail addresses will not be issued to students. Students will not be allowed to use 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 computers, computer 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 computers and computer 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 ***will*** monitor any and all aspects of its computers, computer 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 technology coordinator shall have both the authority and right to examine all computer and internet activity including any logs, data, e-mail, computer disks and/or other computer related records of any user of the system. 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 computers and computer network systems, including the internet.

No warranties, expressed or implied, are made by the District for the computer technology and internet access being provided. Although the District has taken measures to implement and maintain protection against the presence of computer viruses, spyware, and malware on the District's computers, computer network systems, and internet access, the District cannot and does not warranty or represent that the District's computers, computer network systems or internet access will be secure and free of computer 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 computers, computer network systems, and/or internet access. Any risk and/or damages resulting from information obtained from the District's computers, computer 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 computers, computer network systems, and the internet.

Every computer in the District having internet access shall not be operated unless internet access from the computer 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 technology coordinator may close a user account at any time as required and 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 computer systems may be denied access to the District's computers, the District's computer network systems, and the internet. Students and staff members will be instructed or provided information by the District's technology coordinator (or designee) on the appropriate use of the District's computers, computer network systems, and the Internet Acceptable Use policy and regulations, that they will comply with the policy and regulations, and that they understand the consequences for violation of the policy or regulations.

In compliance with federal law, this policy will be maintained at least five years beyond the termination of funding under the Children's Internet Protection Act (CIPA) or E-rate. The interpretation, application, and modification of this policy are within the sole discretion of the Clinton 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.