INTERNET AND COMPUTER NETWORK-APPROPRIATE USE AND SAFETY

Because technology is a vital part of the school district curriculum, the Internet and an internal computer network will be made available to employees and students. Appropriate and equitable use of these resources will allow employees and students to access resources unavailable through traditional means. This Policy is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, ensure technology access is used for educational and district related purposes, and to comply with the Children's Internet Protection Act ("CIPA") and the Children's Online Privacy Protection Act ("COPPA").

Students will be able to access the Internet and other network resources at the discretion of their teachers. Individual student network accounts, Google Apps for Education accounts, and electronic mail addresses will be issued to students in grades 2-12. Additionally, teachers periodically use other online tools with students as needed to achieve their curricular objectives. Parents who wish to prevent their student from accessing online tools using accounts provided by the district must complete the appropriate opt out form available from their child's school. Access to the district's network is provided via an assigned username and password for middle and high school students and all staff. It is the responsibility of users to maintain the privacy of their password. Users should never give out their account credentials under any circumstances and should never reply to an unsolicited email seeking account credentials or other personal information.

The Internet can provide a vast collection of educational resources for students and employees. It is a global network which makes it impossible to control all available information. Because information appears, disappears and changes constantly, it is not possible to predict or control what students may locate. The school district makes no guarantees as to the accuracy of information received on the Internet. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students might encounter information that may not be of educational value. Student Internet records and access records are confidential records treated like other student records. The district will use technology protection measures to block or filter, to the extent practical, access of material which is obscene, pornographic, and harmful to others over the network. The district reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of district property, network, and/or Internet access or files, including email, as district email may be a public record.

Students at all ages will be engaged in age-appropriate instruction on internet safety and appropriate online behavior, including interacting with other individuals on social networking sites and chat rooms. This will include awareness and appropriate response to cyber bullying. The foundations for this instruction are found in our Media Standard 3: Seeks multiple perspectives, shares information and ideas with others and uses information and resources ethically, Objective 8: Follows Internet safety rules and guidelines as outlined in policy and OnGuard Online curriculum.

The network is to be used in support of education and research and consistent with the purposes of the Waterloo Community Schools District. It is not to be used for commercial or for-profit purposes, and should not be used extensively for personal and private business. Additionally, the network should not be used for product advertisement or political lobbying. Users must not use the network to access or process pornographic material, threatening or obscene material, inappropriate files, or files dangerous to the integrity of the network. Additionally, hate mail, harassment, discriminatory remarks, or other antisocial behaviors must not be used on the network, and copyright laws must not be violated. Users must not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network. As the use of the internet and the district's network is a privilege, inappropriate use may result in cancellation of those privileges and may also lead to disciplinary and/or legal action for both students and employees.

Staff members may be given access to confidential or protected information through the district's information systems or through other mediums. Staff cannot disclose this information to any outside individual or group without consent from technology services or student services. Additionally, staff must only access information relevant to their job function within the Waterloo Community School District. Further, staff must understand that user IDs and passwords are personal keys to provide access to confidential information. These credentials must not be shared with anyone, as staff members are liable for information retrieved, altered, or shared from their account.

Staff members should also take appropriate measures to protect and safeguard confidential data they create, modify, or access. Confidential information, such as but not limited to social security numbers and bank account information, should never be stored on removable media such as flash drives. Staff should also ensure that confidential information is never transmitted over insecure or unencrypted mediums. If there is any question whether a medium, service, or site is secure, staff members should consult with technology services. The staff member sharing data is responsible for ensuring only relevant individuals can access the data being shared. Staff should take particular caution when sharing data via cloud-based services to ensure they have set security permissions appropriately to restrict access to confidential information. Any suspected data breaches should be reported immediately to the staff member's supervisor and to technology services.

Legal Ref.: Iowa Code § 279.8 (2013).

Cross Ref.: 504.3 Student Conduct Code
506.3 Student Records Access
506.31 Student Library Circulation Records
506.4 Student Directory Information
603.9 Use of Instructional Technology
704.5 Copyright Policy

ADOPTED: 06/17/96
10/17/96
01/12/09
1/9/12
8/25/14
3/7/16

Reviewed: 5/96, 10/26/98, 3/2/01, 10/7/04, 11/06/08, 12/1/11, 8/1/14, 2/4/16