Access to District Technology, Network Systems, and Internet Access

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. 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.

Parents/guardians may request in writing that their child's connection to the Internet be restricted. Some educational content, resources, and assessments are only available via the District's data network and Internet connection. Students who are restricted will still use those educational resources deemed essential by the District.

Protecting and Monitoring District Technology

The District will have procedures that govern access, use and security of the District networked resources in order to exercise appropriate control over computer records, including financial, personnel and student information. The procedures will address: role-based access, remote access, passwords, system administration, data back-up (including archiving of e-mail), and disaster recovery.

The District's system administrators may close a user account at any time, and administrators may request the system administrators 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/or the District's internet access

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 and electronic files. The administration 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 and other communication tools are limited to District and educational purposes only. Students and employees 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.

Internet Content Filtering

The internet is an ever-expanding resource that adds large quantities of content on a daily basis. While the internet is an extremely valuable tool for learning, some of the content is inappropriate for student use and may even be harmful to students' health, safety and welfare. Therefore, the District has determined that it will limit student access to certain undesirable topics, including but not limited to, information and images that are obscene, constitute child pornography or are otherwise harmful to minors. Since it is not feasible for the District to continually monitor the content of the internet, the District will employ technology protection measures in the form of internet filtering software or services in an attempt to block access to these types of harmful and inappropriate materials.

The District's implementation of internet filtering does not guarantee that students will be prevented from accessing materials that may be considered inappropriate and/or harmful. However, it is a meaningful effort on the part of the District to prevent students from accessing inappropriate and/or harmful materials on the internet. The District makes no guarantee that the filtering software will be available at all times or that the filtering software will block all inappropriate and/or harmful material.

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.

If there is an accessible Uniform Resource Locator [URL] that may be inappropriate and not blocked, or if an educationally valuable URL is blocked, staff may submit a request to have the site reviewed and the filtering of that site changed (blocked or unblocked). All requests are submitted via the Web Filtering Request at http://www.cr.k12.ia.us/district-resources/technology/. All requests to change filtering status of a URL will be logged.

Cross Reference: Regulation 503.2

Approved: 06-11-18
Revised: 04-27-2020