ELECTRONIC RESOURCES AND INTERNET SAFETY

The board of directors recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that staff and students need to be proficient and safe users of information, media, and technology to succeed in a digital world.

Therefore, the district will develop and use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways and for staff to educate them in such areas of need. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings use these tools. The district's technology will enable educators and students to communicate, learn, share, collaborate and create; to think and solve problems; to manage their work; and to take ownership of their lives.

The superintendent or designee will create electronic resources and develop related educational systems that support innovative teaching and learning and provide appropriate staff development opportunities. To promote Internet safety and appropriate online behavior of students and staff as they use electronic resources and access material from the Internet, the superintendent or designee is authorized to develop or adopt Internet safety policies and procedures and acceptable use guidelines. The superintendent or designee in evaluating such procedures and instructional materials should take into account District electronic resources, community norms, privacy rights, responsible use, and issues of concern with student or staff use of electronic resources.

As a component of district Internet safety measures, all district-owned electronic resources, including computer networks and Wi-Fi, in all district facilities capable of accessing the Internet must use filtering software to prevent access to objectionable materials including but not limited to obscene, racist, hateful or violent material. However, given the ever-changing nature of the Internet, the district cannot ensure that a student will never be able to access objectionable material.

Consistent with the federal Children's Internet Protection Act (CIPA), the district will address the following issues regarding Internet safety:

- Preventing access by students to inappropriate and harmful matter on the Internet and World Wide Web;

- Providing for the safety and security of students when using electronic resources.

- Prohibiting unauthorized access, including so-called "hacking" and other unlawful activities by students online.

- Preventing unauthorized disclosure, use, and dissemination of personal information regarding minors.

The district will use the following four-part approach to Internet safety.

1. Network Use Agreement: Any student or staff member using the Internet from a computer in the district facility must have a valid network use agreement on file.

2. Filter: All district-owned computers in all district facilities capable of accessing the Internet, and all district-operated networks providing access to the Internet (such as Wi-Fi), must use filtering software to prevent access to visual depictions that are obscene, child pornography, or, with respect to the use of computers by students, harmful to minors.

3. Supervision: When students use the Internet from school facilities, district staff will make a reasonable effort to supervise student access and use of the Internet. If material is accessed that violates standards in the district's procedures governing network or student guidelines for electronic resources or acceptable use, district staff will instruct the person to cease using that material and/or implement sanctions consistent with district policies, procedures, guidelines, or student codes of conduct.

4. Instruction: Students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The board directs the superintendent to develop regulations that implement the above approach and encourage responsible access to electronic information networks by students while establishing reasonable controls for the lawful, efficient, and appropriate management of the system.

Legal Reference:	18 U.S.C. §§ 2510-2522	Electronic Communication Privacy Act
	47 C.F.R. § 54.520	Children's Internet Protection Act (CIPA)
Management Resources:	*Policy News*, June 2008	Policy News
	Policy News, June 2001	Congress Requires Internet Blocking at School
	Policy News, August 1998	Permission required to review e-mail
Cross References:	Policy 2020	Curriculum Development and Adoption of Instructional Materials
	Policy 2025	Copyright Compliance
	Policy 3207	Prohibition of Hazing, Harassment, Bullying, Threats, Assault, Intimidation, Illegal Discrimination
	Policy 3241	Classroom Management, Corrective Actions and Punishment
	Policy 3245	Students and Telecommunication Devices Procedure
	Policy 3600	Student Records
	Policy 4040	Public Access to District Records
	Policy 4400	Election Activities
	Policy 5710	Internet and Other Electronic Information Networks

Initially Adopted: February 13, 1995
Adopted: October 26, 2009
Amended: April 9, 2012
Amended: April 27, 2015

Amended: April 9, 2018