For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

TSD provides for a system of computers and voice and data networks, including the Internet, to promote educational excellence, to promote resource sharing, to promote innovative instruction and communication, and to prepare students to live and work in the 21st century. The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administration purposes.

AVAILABILITY OF ACCESS

Access to the School's technology resources, including the Internet, shall be made available to students, employees, and other authorized users primarily for educational and administrative purposes and in accordance with administrative regulations.

LIMITED PERSONAL USE

Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the School;
2. Does not unduly burden the School's technology resources;
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

USE BY MEMBERS OF THE PUBLIC

Access to the School's technology resources, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's technology resources.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purpose and mission of the School and with applicable laws and policies.

Access to the School's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges regardless of whether any other disciplinary action is taken. Violations of law may result in criminal prosecution as well as disciplinary action by the School.

SOCIAL MEDIA

The use of social media including social networking sites, such as Facebook, Twitter, Instagram, LinkedIn and others, and video sharing web sites such as YouTube and others, shall adhere to the School's "Social Media Guidelines" on TSD's website.

STUDENT PARTICIPATION IN SOCIAL MEDIA

Under appropriate system controls and supervision, participation in approved social media using the School's technology resources for educational and administrative purposes is permissible for students and staff. Students participating in social media using the School's technology resources should assume that all content shared, including pictures is public. No personally identifying information should be published. Students should not respond to requests for personally identifying information or contacts from unknown individuals.

INTERNET SAFETY

The Superintendent or designee shall develop, implement, and annually review an Internet safety plan to:

1. Control students' and employees' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyber bullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms.

FILTERING

The School shall have an Internet filtering device or software that can block access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

MONITORED USE

Electronic mail transmissions and other use of the School's technology resources by students, employees, and members of the public shall not be considered private. Designated School staff

shall be authorized to monitor such communication at any time to ensure appropriate use.

PERSONAL TECHNOLOGY RESOURCES

Students, employees and guests may connect personal technology resources to the School's network for educational purposes as set forth by the Superintendent or designee.

SOFTWARE

All software used in the School must be legally licensed and approved. All School-funded software shall be approved and installed by technology department staff or a designee.

DONATED RESOURCES

Donated technology resources may be accepted if the equipment and or software meets or exceeds the minimum standards as set forth by the Superintendent or designee. All donated technology resources shall become the property of the School

DISCLAIMER OF LIABILITY

The School shall not be liable for users' inappropriate use of the School's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The School shall not be responsible for ensuring the availability of the School's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

RECORD RETENTION

A School employee shall retain electronic records, whether created or maintained using the School's technology resources or using personal technology resources, in accordance with the School's record management program.

SECURITY BREACH NOTIFICATION

Upon discovering or receiving notification of a breach of system security, the School shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The School shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the School has electronic mail addresses for the affected persons.
3. Conspicuous posting on the School's Web site.
4. Publication through broadcast media.

ESEA Funding

No federal funds made available under Title IV, Part A of the ESEA for an elementary or secondary school that does not receive universal service discount rates may be used to purchase computers used to access the internet, or to pay for direct costs associated with accessing the internet unless the School:

1. Has in place a policy of internet safety for minors that includes the operation of a technology protection measure that protects against access to visual depictions that are

obscene, child pornography, or harmful to minors; and enforces the operation of the technology protection measure during any use by minors of its computers with internet access; and

2. Has in place a policy of internet safety that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography; and enforces the operation of the technology protection measure during any use of its computers with internet access.

An administrator, supervisor, or other person authorized by the School may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

The School shall certify its compliance with these requirements during each annual program application cycle under the ESEA.

20 U.S.C. 7131

Adopted:	02-06-87	Reviewed:	02-11-16	Amended:	08-16-91	07-02-10
					10-09-98	08-10-12
					08-28-99	12-14-12
					10-13-00	02-16-17
					08-10-01	08-25-17
					03-05-04	04-30-21