POLICIES PERTAINING TO OUR BOARD OF DIRECTORS

TECHNOLOGY RESOURCES

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment. "Technology protection measure" means a specific technology that blocks or filters Internet access.

PEIMS:

The District shall participate in the Public Education Information Management System (PEIMS) and through that system shall provide information required for the administration of the Foundation School program and of other appropriate provisions of the Education Code. The PEIM data standards, established by the Commissioner, shall be used by the District to submit information.

CHILDREN'S INTERNET PROTECTION ACT:

The Children's Internet Protection Act (CIPA) addresses concerns about access to offensive content over the Internet on school and library computers. In early 2001, the FCC issued rules implementing CIPA. Schools subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors.)

CERTIFICATIONS:

Under the Children's Internet Protection Act, the District must, as a prerequisite to receiving universal service discount rates, implement certain Interne safety measures and submit certification the Federal Communications Commission (FCC).
(See CERTIFICATION TO FCC, below, for details)

Districts that do not receive universal service discounts but do receive certain federal funds under the Elementary and Secondary Education (ESEA) must, as a prerequisite to receiving their funds, implement certain Internet safety measures and submit certification the Department of Education (DOE). (See ESEA FUNDING, below, for details)

AVAILABILITY OF ACCESS:

Access to the District's technology resources, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

LIMITED PERSONAL USE:

Limited personal use of the District's technology resources shall be permitted if the use:

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

USE BY MEMBER OF THE PUBLIC:

Access to the District'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 purposes and mission of the District and with law and policy.

Access to the District'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 and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

TECHNOLOGY PROTECTION MEASURE:

In accordance with the appropriate certification, the District shall operate a technology protection measure that protects minors against access to visual depictions that are obscene, child pornography, or harmful to minors; and protects adults against access to visual depictions that are obscene or child pornography.

INTERNET SAFETY:

The Superintendent or designee shall develop and implement an Internet Safety Policy Plan that address:

1) Control of students' access to inappropriate materials, as well as to materials that are harmful to minors;
2) Assurance of 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.

PUBLIC HEARING:

After the Superintendent or her/his designee develops an Internet Safety Plan, the District Internet safety policy, the District shall provide reasonable notice and hold at least one public hearing or meeting to address the proposal. After public input, the proposal shall be presented to the Board for final approval.

FILTERING:

Each District computer with Internet access and the District's network systems shall have filtering devices or software that blocks 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 (CIPA) 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 District's technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

DISCLAIMER OF LIABIILTY:

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

RECORD RETENTION:

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

CERTIFICATION TO THE FCC:

To be eligible for universal service discount rates, the District shall certify to the FCC during each annual program application cycle, in the manner prescribed at 47 CFR 54.520, that:

1) An Internet safety policy has been adopted and implemented.

2) With respect to use by minors, the District is enforcing the Internet safety policy, educating minors about appropriate online behavior as part of its Internet safety policy, and operating a technology protection measure during any use of the computers.

3) With respect to use by adults, the District is enforcing an Internet safety policy and operating a technology protection measure during any use of the computers.

ESEA FUNDING:

Federal funds made available under Title II, Part D of the ESEA for an elementary or secondary school that does not receive universal service discount rates may not be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet Unless the District:

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.

CERTIFICATION TO DOE:

The District shall certify its compliance with these requirements to the Department of Education (DOE) as part of the annual application process for each program funding year under the ESEA. To be eligible for universal service discount rates, the District shall certify to the FCC during each annual program application cycle, in the manner prescribed at 47 CFR 54.520, that security breach.

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

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

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

Date Adopted: April 28,2012
Board Approval: (Pending)