PROPOSED REVISIONS
Update 114 Revisions

Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

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

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 Members 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. [See CY(LOCAL) for copyright issues]

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. [See DH(LOCAL), FN series, FO series, and

the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Internet Safety

The Superintendent ~~or designee~~ shall develop and implement an internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications including understanding privacy issues, "netiquette," identifying violence and hate sites, and understanding social sites;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students;
5. Identify parent responsibilities to set rules and guidelines, discuss risks of inappropriate use, monitor access, and look for symptoms of dangerous usage at home; and
6. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

The District's network systems shall have filtering devices that block access to text or 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 consider not filtering specific websites 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 and may be subject to disclosure as specified by the Public Information Act.

Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

Disclaimer of Liability

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 for District business, in accordance with the District's record management program. [See CPC]

ELECTRONICALLY SIGNED DOCUMENTS

AT THE DISTRICT'S DISCRETION, THE DISTRICT MAY MAKE CERTAIN TRANSACTIONS AVAILABLE ONLINE, INCLUDING STUDENT ADMISSIONS DOCUMENTS, STUDENT GRADE AND PERFORMANCE INFORMATION, CONTRACTS FOR GOODS AND SERVICES, AND EMPLOYMENT DOCUMENTS.

TO THE EXTENT THE DISTRICT OFFERS TRANSACTIONS ELECTRONICALLY, THE DISTRICT MAY ACCEPT ELECTRONIC SIGNATURES IN ACCORDANCE WITH THIS POLICY.

WHEN ACCEPTING ELECTRONICALLY SIGNED DOCUMENTS OR DIGITAL SIGNATURES, THE DISTRICT SHALL COMPLY WITH RULES ADOPTED BY THE DEPARTMENT OF INFORMATION RESOURCES, TO THE EXTENT PRACTICABLE, TO:

- **AUTHENTICATE A DIGITAL SIGNATURE FOR A WRITTEN ELECTRONIC COMMUNICATION SENT TO THE DISTRICT;**
- **MAINTAIN ALL RECORDS AS REQUIRED BY LAW;**
- **ENSURE THAT RECORDS ARE CREATED AND MAINTAINED IN A SECURE ENVIRONMENT;**
- **MAINTAIN APPROPRIATE INTERNAL CONTROLS ON THE USE OF ELECTRONIC SIGNATURES;**
- **IMPLEMENT MEANS OF CONFIRMING TRANSACTIONS; AND**
- **TRAIN STAFF ON RELATED PROCEDURES AS NECESSARY.**

~~**Security Breach Notification**~~

~~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 website.~~

~~Publication through broadcast media.~~