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, employees, and members of the community primarily for instructional and administrative purposes and in accordance with administrative regulations. All users shall be prohibited from using network resources for personal gain or commercial work.

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;
3. Has no adverse effect on an employee's job performance or on a student's academic performance; and
4. Has no commercial purpose.

Use by Members of the Public

If possible, and in accordance with administrative regulations, members of the District community may use the District's electronic communications systems, computers, the internet, other technology resources, and software for education- or District-related activities, as long as the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources;
3. Does not hamper the primary mission of technology for students and staff; and
4. Has no commercial purpose.

Denial of Access

Any user identified as a security risk or as having improperly used the District's technology resources or violating District and/or campus acceptable use policies or administrative regulations may be denied access to the system.

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations and user agreements, consistent with the purposes and mission of the District. District services may not be used for any activity that contravenes the law of the United States or any other applicable jurisdiction.

All users shall be required to acknowledge receipt and understanding of administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of use and compliance with such regulations.

Noncompliance may result in suspension of access, termination of privileges, and other disciplinary action consistent with District policies, the Student Code of Conduct, and administrative regulations. [See DH, FN series, FO series] Disciplinary measures may also require restitution for costs associated with technology resource restoration or hardware or software costs. Violations of law may result in criminal prosecution.

Security and Safety

The District shall provide a filtering service that attempts to block access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors as defined by the Children's Internet Protection Act or any other applicable laws, as well as determined by the Superintendent or designee.

The Superintendent or designee shall enforce such services. Upon approval from the Superintendent or designee, an authorized person may grant access for bona fide research or other lawful purpose.

Internet Safety Training

The District shall permit user access to the internet in accordance with law, policy, and administrative regulations.

The District shall provide internet safety training to students no later than the end of the first six weeks of instruction. Training shall include a review of the rules in the student handbook and in the Student Code of Conduct concerning cyberbullying, chatting, inappropriate use of social networking sites, and other technology-related issues.

Levels of Access

Additional levels of access to technology resources shall be granted by the administrator of the system based on administrative and instructional roles. Any attempt to access technology resources for which the user has not been specifically granted rights shall result in disciplinary action consistent with policy and administrative regulations.

Technology Resources

The technology resources provided through the District are and shall remain the property of the District. Users of technology resources shall comply with all policies and administrative regulations of the District.

Donated Technology Resources

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

Personal Technology Resources	Students, employees, and guests may connect personal technology resources to the District's guest wireless network as set forth in administrative procedures. Connecting personal technology resources to the District's wired network shall only be allowed with written permission as set forth in administrative procedures.
Software	All software used in the District must be legally licensed and approved as set forth in the administrative regulation governing the software approval process. All District-funded software shall be installed by the technology department staff or designee.
Donated Resources	Software shall be accepted as donations to the District if the software meets the standards outlined in administrative regulations governing the software approval process. All donated software shall become the property of the District and shall be installed by technology department staff or a designee.
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. The District reserves the right to monitor access to and use of email, instant messaging, the internet, or other network or computer-related activity. Monitoring may occur while engaging in routine maintenance, carrying out internal investigations, preparing responses to requests for public records, or disclosing messages, data, or files to law enforcement authorities. Monitoring may occur 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, 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.
4. Publication through broadcast media.