
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 all the District's electronic communication systems and electronic equipment, including, but not limited to, e-mails, text messaging systems, internet access, the District's intranet, and voice mail.

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 the 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;
4. Has no commercial purpose; and
5. Is limited in the same manner as personal use of the District's voice telephone system. An employee shall not use technology resources for personal use while assigned to other duties.

For employee use of District technology equipment not issued to employees, see CMB(LOCAL).

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

Denial of Access

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

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, 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.

Disciplinary measures may require restitution for costs associated with technology resource restoration, hardware, or software.

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;
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 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 shall provide a filtering device or software that attempts to 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.

TECHNOLOGY RESOURCES

CQ
(LOCAL)

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

Personal Technology Resources

Students, employees, and guests may connect personal technology resources to the District network for educational purposes as set forth by the Superintendent or designee. [See FNCE for student use of personal electronic devices for instructional purposes.]

Software

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

Donated Resources

Donated technology resources may 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.

Donated Software Resources

Software may be accepted as a donation to the District if the software meets the standards as set forth by the Superintendent or designee. 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. 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, 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.

**Transfer of
Equipment to
Students**

At the end of the school year in which the equipment is transferred to the student, the District may determine that the surplus equipment no longer has market value and is not required to be returned to the District.

All students who do not have a computer at home shall be eligible for equipment.

Guidelines for
Transfer of
Equipment to
Students

As used in these guidelines, the term "transfer" does not necessarily imply permanent ownership.

Transfer of equipment under these guidelines does not commit the District to provide internet access or remote access to the District's electronic network from a student's residence.

Before equipment may be transferred under these guidelines, the District shall make a determination that such a transfer serves a public purpose and benefits the District.

Equipment may be transferred under the following conditions:

1. The District shall re-image the computer equipment in order to remove any offensive, confidential, or proprietary information, as determined by the District.
2. An application form shall be completed by the parent or guardian, acknowledging the following:
 - a. There is currently no computer in the student's home.
 - b. The parents understand a mandatory training session is required prior to obtaining the equipment.
 - c. Preference shall be given to educationally disadvantaged students, with the exception of Title I schools, where all students shall be given preference.
 - d. No further training or technical assistance shall be provided.