
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 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. [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.

Internet Safety

The Superintendent 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

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 and as determined by the Superintendent.

The Superintendent shall enforce the use of such filtering devices. Upon approval from the Superintendent, 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 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.

Personal Recording Devices

Personal recording devices shall include camera phones, cameras, audio/tape recorders, video recorders, and any other electronic device capable of recording a human voice or image. Restrictions regarding the use of personal recording devices in District facilities and related activities on or off campus shall include the following:

1. All employees, including student workers, shall be prohibited from using recording devices to duplicate confidential information, including student records, personal records, and medical records. [See CQB, DBA, FFAC, and FL]
2. All employees, students, and visitors shall be prohibited from using recording devices in restrooms, locker rooms, dressing rooms, and other locations where people have a reasonable expectation of privacy.
3. Teachers and instructional personnel shall have the authority to impose restrictions on students regarding the use of recording devices in classrooms, laboratories, and other settings where instruction or testing occurs and shall provide written notification to students on the restrictions with use of recording devices in accordance with this policy. The restrictions shall be included in any syllabus and other District publications, including the student handbook, distributed to students. [See FNCE]

4. All employees shall be prohibited from using recording devices at any District facility or during work-related activities and meetings.

| | |
|------------------------------|---|
| Exception | An employee or student with a disability shall be permitted to use personal recording devices as a reasonable accommodation. An employee requesting such an accommodation shall contact the District's human resources department. A student requesting such an accommodation shall contact student support services. |
| Secret Recordings Prohibited | The District prohibits the secret operation of personal recording devices by employees and students while on District property. This includes, but is not limited to, the use of personal recording devices concealed on or within an individual's person, clothing, or belongings. Additionally, parents of students shall be prohibited from concealing personal recording devices on or within his or her student's person, clothing, or belongings. |
| Notice of Criminal Penalty | The District hereby notifies all employees, students, and parents that, in accordance with the Texas Penal Code, it is a crime to record a conversation to which one is not a party. |
| Confiscation | An authorized District employee shall have the authority to confiscate a personal recording device used in violation of District policy. [See FNCE] |
| Discipline | Violations of the provisions regarding personal recording devices may result in disciplinary action, up to and including termination or expulsion. |