
Note: The Texas Education Agency (TEA), in consultation with the Texas Health and Human Services Commission (HHSC), provides [model health and safety best practice guidelines](#)¹ for the use of digital devices.

Student Access to Digital Technology

The District's use of technology in classrooms and student access to digital devices will be designed to improve student academic performance, and in consideration of student mental and physical well-being.

Student access to digital devices will follow these guidelines:

- A student's use of technology will be intentionally integrated within the District's instructional program and curriculum.
- Technology will be intentionally related to student learning and will only be used when evidence establishes that the integration of technology into the curriculum improves student learning experience and outcomes.
- Screen time and technology exposure over the course of the instructional day, week, and unit will be used for the benefit of the students' learning experience.

Cell Phones

Cell phone usage by a student will not be permitted during the school day, unless the student has approval for the use by a District or campus administrator.

Social Media

A student will not have access to social media platforms during the school day, unless approved by a District or campus administrator.

Note: The Texas Department of Information Resources (DIR) provides guidance about [covered applications and prohibited technology](#)² to address Government Code Chapter 620, which requires governmental entities to ban any "covered applications" developed or provided by the company ByteDance Limited, including the social media service TikTok.

Prohibited Applications on District-Owned Devices

The use or installation of a "covered application," as defined by state law and this regulation, is prohibited on any device owned or leased by the District [see CQC(LEGAL)]. This applies to all full-time and part-time District employees, contractors, and users of District technology resources.

Devices include, but are not limited to, cell phones, tablets, desktop and laptop computers, and any other internet-capable devices.

	The Superintendent is authorized to designate other software or applications as covered applications for purposes of this regulation.
Procedures to Manage District-Owned Devices	The District will use the following procedures to manage devices owned or leased by the District: • Identify, track, and manage all devices owned or leased by the District; • Prohibit the installation or use of a covered application; and • Remove a covered application, on a device owned or leased by the District.
Security Measures	For all District-owned or -leased devices, the District will have security measures that: • Restrict access to app stores or unauthorized software repositories; • Maintain the District's ability to remotely wipe noncompliant or compromised devices; and • Maintain the District's ability to remotely uninstall unauthorized software from devices.
Exception	Any exception will require approval of the <i>Chief Technology Officer</i> and will be in accordance with state law. If an exception is granted, measures will be taken to mitigate the risk posed to the District during the application's use. Any exception will be documented along with the measures taken to mitigate these risks.
Personal Devices	The District prohibits use of covered applications on any personal devices that are used to conduct District business on the District network.
Acknowledgment of Regulation	Annually, each employee will receive notice of this regulation and provide documentation that they have received this regulation.

¹Texas Education Agency, Technology Guidance: <https://tea.texas.gov/texas-schools/school-boards/hb-3489-guidance-updated.pdf>

²Texas Department of Information Resources, Covered Applications and Prohibited Technologies: <https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies>