



**WINDHAM SCHOOL
DISTRICT**

NUMBER: SD-10.20
DATE: February 15, 2023
PAGE: 1 of 4
SUPERSEDES: N/A

SUPERINTENDENT DIRECTIVE

SUBJECT: PROHIBITED TECHNOLOGIES

AUTHORITY: Windham Board Policy BP-03.01, “WSD Superintendent Responsibilities and Authority;” Statewide Plan for Preventing Use of Prohibited Technology in State Agencies (texas.gov)

Reference: Windham Superintendent Directive SD-10.13, “Information Resources Security”

APPLICABILITY: Windham School District (WSD)

POLICY:

To provide protection against technological threats to the state’s sensitive information and critical infrastructure, Windham School District (WSD) prohibits the use of hardware, equipment, software, applications, and websites designated as prohibited technologies. Prohibited technologies may not be used on state-owned devices or personal devices used to conduct state business, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

DEFINITIONS:

The following terms are defined for the purpose of this directive and are not intended to be applicable to other policies or procedures.

“Information Resources” (IR) means the procedures, equipment, or software that are employed, designed, built, operated, or maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

“Sensitive location” is any location, physical or logical (such as video conferencing, or electronic meeting rooms), that is used to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

“Unauthorized Devices” means any state-owned device or personal device used to conduct state business that includes any prohibited hardware or software.

“User” is any employee, contract employee, consultant, vendor, intern, or volunteer authorized to access the IR by the information owner, in accordance with the owner’s procedures and rules.


PROCEDURES:

I. General Guidelines

- A. WSD and the Texas Department of Criminal Justice (TDCJ) will implement the removal and prohibition of technology listed in Attachment A.
- B. WSD and TDCJ may prohibit technology threats in addition to those identified by the Texas Department of Information Resources (DIR) and the Texas Department of Public Safety (DPS).
- C. TDCJ will configure agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, the TDCJ wide area network (WAN), and virtual private network (VPN) connections.
- D. WSD and TDCJ will prohibit personal devices with prohibited technologies installed from connecting to agency or state technology infrastructure or state data.
- E. WSD will access a separate network provided by TDCJ for access to prohibited technologies with the approval of the WSD superintendent or TDCJ executive director, as applicable.
- F. WSD will identify, track, and control state-owned devices to prohibit the installation of, or access to, prohibited applications for mobile, desktop, or other internet-capable devices.
- G. WSD will manage state-issued mobile devices by:
 - 1. restricting access to “app stores” or non-authorized software repositories to prevent the install of unauthorized applications;
 - 2. maintaining the ability to remotely wipe non-compliant or compromised mobile devices;
 - 3. maintaining the ability to remotely uninstall un-authorized software from mobile devices; and
 - 4. deploying secure baseline configurations for mobile devices, as determined by WSD.

- H. Sensitive locations will be identified, cataloged, and labeled by the WSD.
 - I. Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, including any electronic meeting labeled as a sensitive location.
 - J. All users shall sign a document annually confirming their understanding of this policy.
- II. Exceptions
- A. Exceptions to the ban on prohibited technologies may only be approved by the WSD superintendent or TDCJ executive director, as applicable. This authority may not be delegated. All approved exceptions to statewide prohibited technology must be reported to DIR.
 - B. Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or sharing of information to the public during an emergency. Exceptions for personal devices used for state business should be limited to extenuating circumstances and granted for a pre-defined time period. To the extent practicable, exception-based use should only be performed on devices that are not used for other state business and on non-state networks. Cameras and microphones should be disabled on devices for exception-based use.
- III. Enforcement

Violation of this policy may result in disciplinary action in accordance with Windham Board Policy 07.44, "Professional Standards of Conduct and Disciplinary Guidelines." Violations by persons not employed by WSD may result in the person being barred from WSD premises and the termination of relationship with WSD. Additionally, individuals may lose WSD and TDCJ IR access, and may be subject to civil liability and criminal prosecution.



Kristina J. Hartman, Ed.S.
Superintendent
Windham School District

The following list of prohibited technologies is current as of January 23, 2023. The up-to-date list is published on the DIR website at <https://dir.texas.gov/information-security/prohibitedtechnologies>.

Prohibited Software, Applications, and Developers

- TikTok;
- Kaspersky;
- ByteDance Ltd.;
- Tencent Holdings Ltd.;
- Alipay;
- CamScanner;
- QQ Wallet;
- SHAREit;
- VMate;
- WeChat;
- WeChat Pay;
- WPS Office; and
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware and Equipment Manufacturers

- Huawei Technologies Company;
- ZTE Corporation;
- Hangzhou Hikvision Digital Technology Company;
- Dahua Technology Company;
- SZ DJI Technology Company;
- Hytera Communications Corporation; and
- Any subsidiary or affiliate of an entity list above.