C.01.09.02 (Procedure) Prohibited Technology Use
Responsible Department: Planning, Performance and Information Systems
Approved: 6-16-26

Employees, contractors, interns, consultants, and any other users of Alamo Colleges District ("ACD") technology resources shall comply with the following procedures governing prohibited technology use on ACD-owned devices, systems, infrastructure, and networks. These procedures are established to protect confidentiality, integrity, and availability of ACD information resources, sensitive information, and critical infrastructure from cybersecurity and operational risks associated with prohibited technologies.

The following prohibited applications, software, services, developers, hardware, equipment, and manufacturers shall not be downloaded, installed, accessed, connected, operated, or otherwise utilized on any ACD-issued device or while conducting ACD business on personal devices.

Prohibited Software/Applications/Developers

***This list includes the board-approved prohibited technologies and additions maintained by Texas Department of Information Resources (DIR)**

- Alibaba
- Alipay
- Baichuan/Beijing Baichuan Intelligent Technology Co. Ltd.
- Baidu
- Beijing Academy of Artificial Intelligence
- ByteDance Ltd.
- CamScanner
- CloudWalk Technology
- DeepSeek
- iFlytek
- Kaspersky
- Lemon8
- Megvii/Megvii Technology Limited
- MiniMax
- Moomoo
- Moonshot AI
- QQ Wallet
- RedNote
- SenseTime/SenseTime Group
- SHAREit
- Shein
- StepFun
- PDD Holdings (including Temu and Pinduoduo)
- Tencent Holdings Ltd.
- Tiger Brokers
- TikTok
- Uniview/Zhejiang Uniview Technologies Co. Ltd.
- VMate
- WeBull

- WeChat
- WeChat Pay
- WPS Office
- Xiaomi
- Yitu Technology
- Zhipu/Z.ai
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers

- Autel Robotics
- CATL/Contemporary Amperex Technology Co. Ltd.
- Dahua Technology Company
- Gotion/Gouxuan Hi-Tech Co. Ltd.
- Hisense Group Co. Ltd.
- Huawei Technologies Company
- Hangzhou Hikvision Digital Technology Company
- Hytera Communications Corporation
- NucTech/Tongfang NucTech Technology Ltd.
- RoboSense Technology Co. Ltd.
- SZ DJI Technology Company
- TCL Technology Group Corp.
- TP-Link
- Uniview/Zhejiang Uniview Technologies Co. Ltd.
- Wuhan Geosun Navigation Technology Co. Ltd.
- Xiaomi
- ZTE Corporation
- Any subsidiary or affiliate of an entity listed above.

Covered Applications

- Lemon8
- RedNote
- TikTok or any successor application or service developed or provided by ByteDance Ltd. or an entity owned by ByteDance Ltd.

Source: https://dir.texas.gov/information-security/covered-applications-and-prohibited-technologies

These procedures apply to all ACD-issued cellular telephones, laptops, tablets, desktop computers, and any other devices capable of internet connectivity, including any personal device utilized to conduct ACD business. ACD business includes accessing ACD-owned or managed data, applications, electronic mail accounts, or non-public communications systems.

C.01.09.02 (Procedure) Prohibited Technology Use
Responsible Department: Planning, Performance and Information Systems
Approved: 6-16-26

Employees and contractors utilizing personal devices for ACD business purposes shall ensure prohibited technologies are not installed, enabled, or accessible on such devices prior to connecting to ACD systems, infrastructure, applications, or data resources.

Planning, Performance and Information Systems ("PPIS"), Information Technology, and Information Security personnel shall maintain, review, and update the prohibited technologies inventory as necessary to address cybersecurity threats, legal requirements, regulatory obligations, or institutional risk management considerations.

ACD shall implement administrative safeguards to prevent the acquisition or renewal of prohibited technologies. Prior to any issuance of purchase order or contract execution, ACD shall verify all vendor bids and purchasing requests against the Texas DIR Prohibited Technologies List.

ACD shall implement administrative, technical, and physical safeguards intended to prevent prohibited technologies from accessing or interacting with ACD information technology infrastructure, networks, systems, or data resources. Such safeguards may include, but shall not be limited to:

- Network access restrictions;
- Network-level Application and domain filtering;
- Endpoint monitoring and detection controls;
- Device authentication requirements; and
- Access denial or quarantine mechanisms.

By policy, users shall not connect or attempt to connect personal devices containing prohibited technologies to ACD-owned or managed networks, systems, applications, infrastructure or data resources. ACD reserves the right to suspend, restrict, monitor, or terminate access for any device determined to be noncompliant with these procedures.

ACD shall maintain enhanced security protections for designated sensitive locations. Sensitive locations may include physical or logical environments utilized to discuss, process, access, transmit, or store confidential, restricted, regulated, or otherwise protected information, including:

- Information technology configurations;
- Criminal justice information;
- Financial information;
- Personally identifiable information;
- Sensitive personal information; and
- Information protected by federal or state law.

ACD shall maintain enhanced security protections for designated sensitive locations. Sensitive locations shall be identified, cataloged, and labeled by ACD. Sensitive locations may include physical or logical environments (such as video conferencing or electronic meeting rooms)

utilized to discuss, process, access, transmit, or store confidential, restricted, regulated, or otherwise protected information, including:

- Information technology configurations
- Criminal justice information
- Financial information
- Personally identifiable information
- Sensitive personal information
- Information protected by federal or state law

The ACD primary and backup data centers are labeled with physical signage and restricted by multi-factor authentication (MFA) and policy to authorized personnel only who receive special training on working with sensitive data. Access to all sensitive locations shall be restricted to authorized personnel and may require MFA, specialized security training, or other security controls deemed appropriate by ACD. Only pre-approved devices shall be permitted within the data centers and other sensitive locations, and use is restricted to a limited basis. Unauthorized devices, including personal cellular telephones, tablets, laptops, wearable technology, or similar electronic devices, shall be prohibited from entering or operating within designated sensitive locations, including any electronic meetings identified as sensitive.

Students may utilize prohibited technologies on privately owned or privately leased personal devices when utilizing an ACD-issued student electronic mail account or other student-authorized services. ACD shall implement reasonable safeguards intended to minimize risks associated with student use of prohibited technologies on personal devices.

Exceptions to these procedures may only be approved by the Chancellor to support law enforcement investigations or other legitimate business purposes. Such authority shall not be delegated.

Requests for exceptions shall:

- Be submitted in writing;
- Include sufficient business justification;
- Identify the prohibited technology involved;
- Specify the intended use and duration; and
- Identify proposed mitigating security controls.

Devices granted an approved exception shall:

- Be utilized solely for the approved business purpose;
- Operate only on designated separate or non-state networks when feasible; and
- Have cameras, microphones, geolocation services, or similar monitoring features disabled whenever not actively required for the approved use case, when technically feasible.

Exceptions involving personal devices shall be limited to extenuating circumstances and approved only for a defined and limited duration.

Failure to comply with these procedures may result in suspension or revocation of access privileges, corrective or disciplinary action, removal of unauthorized devices, termination of contractual relationships, or other administrative action deemed appropriate by ACD.

Reference:

Model Security Plan for Prohibited Technologies
Covered Applications and Prohibited Technologies
Government Code Chapter 620
Senate Bill 1893