C.09.02 (Policy) Prohibited Technology Use
Responsible Department: Planning, Performance and Information Systems
Board Adoption: 08-20-24

Employees and contractors may not download, install, or use the following prohibited applications or technologies on any device issued by Alamo Colleges District (ACD). This includes all ACD-issued cell phones, laptops, tablets, desktop computers, or any other devices capable of internet connectivity. This plan applies to all employees, contractors, interns, or any users of ACD-owned networks. Employees and contractors are banned from conducting ACD business on prohibited technology-enabled personal devices. ACD business includes accessing any ACD-owned data, applications, email accounts, or non-public facing communications.

Prohibited Software/Applications/Developers

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office

Prohibited Hardware/Equipment/Manufacturers

- Huawei Technologies Company
- ZTE Corporation
- Dahua Technology Company
- SZ DJI Technology Company
- Hytera Communications Corporation

Exceptions to this policy are extended to students to accommodate student use if an ACD email address was provided by the District. This exception shall be restricted to student use of a personal device that is privately owned or leased by the student or a member of the student's immediate family, and shall include network security considerations to protect the ACD network and data from traffic related to prohibited technologies.

ACD will implement network-based restrictions to prevent the use of prohibited technologies on ACD networks by any prohibited device.

ACD prohibits personal devices with prohibited technologies installed from connecting or attempting to connect to ACD technology infrastructure or data.

C.09.02 (Policy) Prohibited Technology Use
Responsible Department: Planning, Performance and Information Systems
Board Adoption: 08-20-24

ACD maintains enhanced security measures for sensitive locations, which are identified, cataloged, and labeled by ACD. A 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.

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. Only pre-approved devices are allowed into the data centers and use is restricted to a limited basis. Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.

ACD will coordinate the incorporation of other technology providers as necessary, including any apps, services, hardware, or software that pose a threat to ACD's sensitive information and critical infrastructure.

Exceptions to this policy may only be approved by the Chancellor to enable law-enforcement investigations or other legitimate business uses. This authority may not be delegated.

Devices granted an exception should only be used for the specific use case in which the exception was granted and only used on non-state or specifically designated separate networks. If possible, cameras and microphones should be disabled on those devices when not in active use for their intended purpose.

For personal devices used for ACD business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time.

Reference:
Model Security Plan for Prohibited Technologies
Version 1.0: January 26, 2023