Wharton County Junior College	ADMINISTRATIVE PROCEDURE MANUAL	
WCJC Title: **Prohibitive Technologies**	Section C: **Business and Support Services**	Page(s): 4
BASED ON BOARD OF TRUSTEES POLICY		
Policy Title: **Technology Resources**	Policy: CR (Legal)	
Subtitle: **Prohibitive Technologies**	Date Drafted: 02/15/2023	

Purpose

Wharton County Junior College (WCJC) will comply with state guidelines related to the ban of TikTok and other prohibited technologies on all College-issued devices and networks.

Background

On December 7, 2022, Governor Greg Abbott issued an executive directive to all state agencies ordering the ban of the video-sharing application TikTok from all state-owned and state-issued devices and networks. This order was enacted due to the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan which provides all state agencies additional guidance regarding the management of personal devices that individuals may use to conduct state business.

This plan applies to all state agencies and institutions of higher education, including their employees, contractors, interns, or any users of state-owned networks. Each agency is responsible for the implementation of the plan as outlined in this document, including any changes to meet specific agency needs.

Prohibited Technologies

The Texas DIR maintains the current list of all prohibited technologies, including both software/applications and hardware/equipment. WCJC regularly reviews this list of prohibited technologies to maintain compliance with all DIR regulations.

All banned software and hardware will be referred to as "prohibited technologies" throughout this administrative procedure.

Procedure

1. Prohibited technologies shall not be downloaded or used on any state-issued device, including all state-issued desktop computers, cell phones, laptops, tablets, or any other device that is capable of internet connectivity. WCJC will strictly enforce this objective through the implementation of the following strategic interventions:

    a. WCJC will identify, track, and control all state-owned devices to prohibit the installation of or access to all prohibited technologies. This includes the various applications for mobile, desktop, or other internet-capable devices.

    b. WCJC will determine if prohibited technologies have been downloaded on state-issued devices and, if so, will immediately remove the application from those devices.

    c. WCJC will configure all network firewalls to block prohibited domains on both the local and virtual private networks.

    d. WCJC will manage all state-issued mobile devices by implementing security controls, to include:

        i. The restriction of access to "app stores" or non-authorized software repositories to prevent the installation of unauthorized applications.

        ii. Maintenance of the ability to remotely wipe non-compliant or compromised mobile devices or to uninstall unauthorized software from these devices.

        iii. Deployment of secure baseline configurations for mobile devices, as deemed appropriate by WCJC leadership.

2. WCJC employees or contractors shall not install, operate, or access any prohibited technologies on a personal device that is also used to conduct state business. For the purposes of this Administrative Procedure, "state business" includes accessing any WCJC or other state-owned data, applications, WCJC email accounts, or non-public facing communications. Examples of state network resources include email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state databases or applications.

    If an agency has a justifiable need to allow the use of personal devices to conduct state business, the agency may establish a "Bring Your Own Device" (BYOD) program with the following considerations:

    a. Ability to manage lost, stolen, or unauthorized devices;

b. Ability to prevent the installation of banned or unauthorized software and the use of unsecure public networks;

c. Ability to manage open records, confidentiality, and privacy-related issues;

d. Ability to create a guest security profile that prevents prohibited technologies from communicating or being downloaded while that security profile is in use; and

e. Ability to remove all state-related business and applications from the personal device before removing the security profile or unenrolling the device from the BYOD program.

WCJC does concede an exception to accommodate student use of their student email address which is provided by the College. This exception is restricted to student's use of a personal device that is privately owned or leased by the student or a member of the student's immediate family, and includes network security considerations to protect the WCJC network and College data from traffic related to prohibited technologies.

Any additional exceptions may only be approved by the WCJC President to enable law-enforcement investigations or other legitimate business uses. This authority may not be delegated. All approved exceptions to allow the use of prohibited technologies must be reported to DIR. 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.

3. WCJC will identify, catalog and label sensitive locations within the College. A "sensitive location" includes any location, physical or virtual, that may be used to discuss confidential or sensitive information, including information technology configurations, emergency operations and/or security plans, protected student records, or any data protected by federal or state law.

   WCJC is responsible for securing all sensitive locations. Sensitive locations on the WCJC campus will be clearly marked with exterior signage. In addition, virtual meetings will be labeled as a sensitive location, when applicable. Unauthorized devices, including personal cell phones, tablets, or laptops, may not enter sensitive locations, including virtual meetings labeled as a sensitive location. Any individual, including employees, contractors, or visitors are subject to the limitations associated with a sensitive area.

4. The Texas DIR Cyber Operations has blocked access to prohibited technologies on the state network. WCJC will implement additional network-based restrictions to prevent communication with prohibited internet services. Restrictions implemented by WCJC

will include:

a. Configuration of WCJC network firewalls to block access to statewide prohibited services on all technology infrastructures, including local area, wide area, and virtual private networks.

b. Restriction of personal devices with prohibited technologies installed from connecting or attempting to connect to WCJC technology infrastructure or any state network/data.

5. To provide protection against ongoing and emerging technology threats to the state's sensitive information and critical infrastructure, technologies will be regularly monitored and evaluated for inclusion into this plan.

   The Texas DPS and Texas DIR will evaluate and monitor technologies that pose a threat to state sensitive information and critical infrastructure. In addition, they will provide recommendations to state leaders on technologies that should be blocked or prohibited statewide.

   Texas DIR will host a site that lists all prohibited technologies including apps, software, hardware, or technology providers that are prohibited. New technologies will be added to the list after consultation between DIR and DPS. DIR will notify agencies in the event the list is amended.

   It is the responsibility of WCJC to implement the removal and prohibition of any offending technology. WCJC reserves the right to add additional software and/or hardware to this policy, above and beyond the list of prohibited technologies identified by Texas DIR.

Revised date: 02/15/2023 (AAA)