

Unauthorized Technology, Software, Hardware, and Configuration Changes

WHO THIS APPLIES TO

This applies to all users of Gulf Coast State College technology and networks, including faculty, staff, and other employees; students; guests and visitors; vendors, contractors, and consultants; and lessees. The approval and request processes described below for purchasing, installing, connecting, and deploying technology on behalf of the College apply specifically to employees. All other users are equally subject to this policy's restrictions on the unauthorized installation, connection, modification, movement, or replacement of College technology.

OVERVIEW

To help protect Gulf Coast State College (GCSC) systems, information, users, and technology infrastructure, you may not install, connect, modify, move, replace, disconnect, or otherwise alter college technology without prior authorization.

This applies to college-owned or managed computers, laptops, mobile devices, televisions, displays, classroom technology, networking equipment, printers, IoT devices, and any other technology connected to or managed by the college.

The purpose of this policy is to prevent unauthorized changes that could introduce security vulnerabilities, interfere with normal operation, expose college information, create unsupported configurations, or bring unmanaged technology into the college environment.

PRIOR APPROVAL REQUIRED

All hardware, peripherals, software, applications, drivers, and other technology must be approved by the Media Services Manager, an ITS Director, or the CIO before it is purchased, installed, connected, deployed, or placed into service.

This applies whether the technology is paid for with college funds, department funds, grant funds, or provided at no cost. Approval is required before you purchase or install, not after the fact.

Examples include, but are not limited to:

- Computers, monitors, docks, adapters, and peripherals
- Printers, scanners, cameras, microphones, and other accessories
- USB devices and removable storage
- Software and applications
- Device drivers and firmware
- Browser extensions and add-ons
- Classroom and presentation technology

- TVs, displays, and digital signage equipment
- Network and wireless equipment
- IoT and smart devices
- Specialized hardware or software used for teaching, research, or administrative purposes

MOVING, DISCONNECTING, OR REPLACING EXISTING TECHNOLOGY

Existing college technology must not be disconnected, replaced, relocated, reconfigured, or otherwise altered without prior ITS authorization.

This includes changes that may seem minor, such as:

- Moving a computer, monitor, TV, display, printer, phone, or other equipment to another location
- Disconnecting existing equipment or cables
- Replacing an existing peripheral with a different model
- Connecting additional equipment to an existing setup
- Moving classroom or presentation equipment
- Changing how equipment is connected to the network
- Removing equipment from its assigned location

Even when a change looks like an improvement or is meant to fix a technical problem, get ITS authorization before making it.

USER-INSTALLABLE SOFTWARE

Most college-managed computers do not give users local administrative access. Even so, many modern applications, utilities, and browser extensions can install inside your user profile without administrative rights.

The fact that software installs without an administrator prompt does **not** mean it is approved for use.

Get the appropriate approval before installing software, drivers, browser extensions, utilities, scripts, or other applications on college-managed devices.

This includes software that:

- Installs without administrative privileges
- Runs from a user's profile or user space
- Is portable and does not require a traditional installation
- Is downloaded directly from the internet
- Operates as a browser extension or add-on
- Modifies, monitors, or adds functionality to a college device

WHY THIS MATTERS

Unauthorized hardware and software can introduce security and operational risks, including:

- Malware or other malicious software
- Unauthorized access or remote access
- Exposure of college information
- Security vulnerabilities
- Network or system instability
- Compatibility issues
- Licensing concerns
- Loss of vendor or manufacturer support
- Difficulty troubleshooting or supporting the technology
- Unmanaged or unknown devices connecting to college systems

Technology does not have to be malicious to cause a security or support problem. Unapproved technology can interfere with existing systems or make it harder for ITS to maintain and secure the environment.

PERSONALLY OWNED TECHNOLOGY

In most cases, you may connect a personally owned device, such as a laptop, phone, or tablet, to the college network for general internet access. The following connection methods are supported:

- Wi-Fi, using the Private Pre-Shared Key (PPSK) assigned to you.
- Wi-Fi, using the shared "Events" password when it is provided for an event.
- The college Guest network.
- Wired (hardwire) connection.

Hardwired personal devices are allowed because the college uses a network access control system. A device that does not authenticate is automatically placed on an internet-only VLAN that is segmented from the college's primary networks. It can reach the internet, but it cannot reach internal college systems or resources.

Connecting a personal device by any of these methods is intended for internet access only. It does not provide or guarantee any ability to interact with, share with, or access other devices, systems, or resources on the same network or on any other college network.

Accessing college email, information, or resources from a personal device is separately governed by the college's Acceptable Use Policy. A personal device used for that access must meet the college's security standards, including current anti-virus, all security updates, device encryption, and a required PIN, passcode, or biometric lock, and it must not be jailbroken or rooted.

Connecting a personal device for internet access is different from the following, which still require prior ITS approval:

- Installing personally owned software on a college-managed device.
- Connecting personal peripherals or storage to a college-managed device.
- Using a personal device to modify, reconfigure, or interfere with college technology.
- Connecting personal networking or wireless equipment, such as routers, switches, access points, or range extenders, to the college network.

ITS may still restrict a personal device that presents a security or operational risk or that does not meet the college's device and security requirements.

COLLEGE TECHNOLOGY AND CLASSROOM EQUIPMENT

College TVs, displays, digital signage, classroom computers, presentation systems, conference room equipment, and other technology are college technology and fall under this policy.

Do not install applications, connect unauthorized hardware, move or disconnect equipment, replace components, or change configurations without prior ITS authorization.

APPROVAL AND REQUESTS

Submit technology needed for teaching, research, administrative work, events, accessibility, or other legitimate college purposes through the appropriate ITS process before purchase or implementation.

ITS may review requests for:

- Security and privacy concerns
- Compatibility with existing systems
- Licensing and procurement requirements
- Vendor support
- Maintenance and lifecycle considerations
- Network and infrastructure impact
- Data access and handling
- Compliance with college requirements

When in doubt, ask ITS before you purchase, install, connect, move, disconnect, or replace technology.

UNAUTHORIZED CHANGES

ITS may remove, disable, disconnect, relocate, or restrict unauthorized hardware, software, drivers, devices, or configurations when they are found.

Where necessary, access to college resources may be restricted until the unauthorized technology or configuration is removed and the system is returned to an approved, supported state.

If unauthorized technology is identified on a device you use, ITS may contact you, and you may be required to work with ITS to resolve it.