FITCHBURG STATE UNIVERSITY

Personal Device Policy

Version 2.0	**Last Updated:** 12/19/2025
Security Level: Public	**Issued:** 10/14/2022

Purpose

Fitchburg State University permits employees and students to use personally owned laptops, tablets, and smartphones to access university technology resources in support of academic, instructional, and administrative activities. This access is a privilege, not a right, and may be revoked at any time.

This policy establishes requirements to protect the confidentiality, integrity, and availability of university data and technology systems while allowing secure and appropriate use of personal devices.

Scope

This policy applies to all members of the Fitchburg State University community, including faculty, staff, students, contractors, affiliates, and any personally owned device that connects to the university network or accesses university systems or data.

Policy

Acceptable Use

Personal device use is permitted solely for legitimate university-related activities that directly or indirectly support the mission and operations of Fitchburg State University.

Personal devices may not be used on the university network to:

- Store, transmit, or process illicit or illegal material
- Harass or threaten others
- Violate the University Acceptable Use Policy or any other university policy

All personal devices must comply with this policy and all applicable institutional, state, and federal regulations.

Device Registration, Authentication, and Network Access

All personal devices must be registered on the university network or authenticated using university-issued credentials prior to accessing university systems or services.

Personal devices are placed on restricted, segmented networks designed to limit exposure to sensitive systems.

Unauthorized, unregistered, or non-compliant devices will be blocked from accessing the University network.

Permitted Devices and Support

The following personal devices are permitted, provided they meet university security requirements:

- Smartphones (e.g., iOS and Android devices) with device-level encryption enabled
- Tablets (e.g., iPads and Android tablets) with device-level encryption enabled
- Laptops that meet minimum security standards as defined by the Technology Department
- Internet-connected (IoT) devices that have up-to-date software/firmware and follow best practices for device security

Support for personal devices is limited to:

- Network connectivity
- Access to university-managed applications and services

Only modern, vendor-supported devices running currently supported operating systems and receiving regular security patches may be used to access university systems or networks. Devices that are outdated, unpatched, or no longer supported by the manufacturer may be denied or blocked from network access until compliance is restored.

The university does not provide hardware repair, operating system troubleshooting, or support for personal applications.

Devices may be required to be presented to the Technology Department for provisioning, security review, or configuration prior to access.

Data Handling and Storage

Personal devices may not store, cache, or locally retain protected university data, including but not limited to:

- FERPA-protected student records
- Personnel or employment data
- Financial or payment card data
- Health or other regulated information

University data must remain within university-approved applications and services that provide appropriate access controls, encryption, and auditing.
It is prohibited to download, export, sync, or back up university data to:

- Personal storage
- Personal cloud services
- Unapproved applications

Approved Applications and Security Controls

Access to university data on personal devices is limited to university-approved applications.
The Technology Department maintains a list of approved applications and services.
The university may enforce application-level controls, including restrictions on:

- File downloads
- Copy/paste functionality
- Screenshots
- Local file storage

Remote Access Removal and Data Wipe

To protect university systems and data, Fitchburg State University reserves the right to remotely remove university-managed applications, sessions, accounts, and data from personal devices when:

- A device is lost or stolen
- An individual separates from the university
- A security incident, policy violation, or malware infection is detected

In limited circumstances where required to protect university systems or data, a full device wipe may be necessary. While reasonable efforts will be made to avoid impacting personal data, the university is not responsible for personal data loss.

The university reserves the right to disconnect devices, disable services, or remove data without prior notice or user approval.

Roles

Users (Faculty, Staff, and Students): Users are responsible for understanding and complying with this policy and all related university policies. They must ensure their personal devices meet the university's security requirements and are used in a manner that protects university data and systems.:

Management: Management is responsible for determining which employees require access to university resources using personal devices. Management must periodically review access authorizations, notify the Technology Department when access needs change, and report suspected policy violations to the Information Security Team.

Technology System Administrators: Technology System Administrators are responsible for registering and authorizing personal devices, enforcing required security configurations and access controls, and ensuring that the university's technology infrastructure is protected from unauthorized access. Suspected violations of this policy must be reported to the Information Security Manager.

Chief Information Security Officer: The Chief Information Security Officer oversees compliance with this policy, ensures it aligns with institutional and regulatory requirements, and periodically reviews and updates the policy as needed.

References

- CIS Critical Security Controls v8
    - Control 1 – Inventory and Control of Enterprise Assets
    - Control 2 – Inventory and Control of Software Assets
    - Control 3 – Data Protection
    - Control 4 – Secure Configuration of Enterprise Assets
    - Control 5 – Account Management
    - Control 12 – Network Infrastructure Management
- University Acceptable Use Policy

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Revision History

Date of Change	Revision	Responsible	Summary of Change
10/14/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
5/9/2024	1.1	Eric Boughton, CISO	Formatting
12/19/2025	2.0	Eric Boughton, CISO Stefan Dodd, CIO	Major revision: CIS alignment, data handling restrictions, device registration, and Role updates.