

# 770.1 IT Asset Disposal and Data Destruction Policy

Policy Title: IT Asset Disposal and Data Destruction Policy

Policy Number: 770.1

Responsible Office: Information Technology Services

Approval Authority: Administrative Council; President's Cabinet (Final Approval)

Applies To: All employees, faculty, staff, students, student workers, contractors, and vendors who manage, handle, store, or dispose of College-owned technology assets.

Alignment: FERPA; GLBA; NIST media sanitization and cybersecurity guidance (as updated)

Effective Date: May 2026

Current Version: 1.0.0

Supersedes: None

Next Scheduled Review: January 2027

## I. Policy Overview and Purpose

This policy establishes standardized procedures for the secure and compliant disposal of College-owned information technology assets. It protects institutional data by ensuring proper sanitization, destruction, documentation, and alignment with applicable legal and regulatory requirements.

## II. Scope

This policy applies to all College-owned or managed technology assets, including devices, storage media, networking equipment, and any hardware capable of storing institutional data.

## III. Definitions

**Sanitization** — A process that renders data on a storage device unrecoverable using certified erasure tools compliant with NIST SP 800-88 Rev. 1.

**Destruction** — Physical destruction of a storage device when sanitization is not technically feasible.

## IV. Data Security and Privacy

To protect institutional data:

- All storage devices must be sanitized using certified data erasure tools prior to disposal.
- Devices containing confidential or restricted institutional data must be physically destroyed if erasure is not feasible.

- Disposal procedures must comply with the Family Educational Rights and Privacy Act (FERPA).

## **V. Disposal Procedure**

### **A. Notification**

Information Technology Services (ITS) is notified when equipment is no longer used or functional and needs disposal.

### **B. Authorization**

Disposal must be approved by the Director of Information Technology Services or designated authority.

### **C. Documentation**

Documentation should include inventory tag, serial number, disposal method, date, and responsible personnel and shall be retained in accordance with the College's Board-approved records retention requirements and applicable retention schedules.

### **D. Assessment**

ITS evaluates whether equipment should be reused, repurposed, donated, recycled, or destroyed.

### **E. Sanitization**

Any device with onboard storage must be wiped using certified erasure methods or have its storage physically destroyed.

### **F. Inventory Tag Removal & Deprovisioning**

- Inventory tag is removed
- Inventory Control is notified
- Device is removed from the College's MDM platform, if applicable

### **G. Secure Storage**

After sanitization, devices are placed in secure storage until donation, recycling, or destruction.

## **VI. Unauthorized Storage**

To maintain inventory integrity and reduce safety and security risks:

- Unused IT assets should not be stored in unauthorized locations such as closets, classrooms, offices, or storage rooms without ITS approval.
- All unused devices must be returned to ITS for proper evaluation and disposition.
- Unauthorized storage may result in data exposure, equipment loss, or safety hazards.
- Periodic inspections may be conducted to identify and recover improperly stored devices.

## VII. Enforcement and Sanctions

Violations of this policy may result in enforcement actions in accordance with the Data Governance and Security Oversight Policy (735.0) and the ITS Enforcement and Escalation Standard (735.0.1).

## VIII. Exceptions

Exceptions must follow the authoritative exceptions framework defined in the Data Governance and Security Oversight Policy (735.0).

## IX. Revisions

This policy shall be reviewed annually to ensure continued accuracy, regulatory compliance, and alignment with institutional practices. Revisions shall follow the College's established approval process, and all individuals are responsible for compliance with the current approved version. Version history shall be maintained in accordance with institutional documentation standards

Version	Date	Description	Approved By
1.0.0	Jan 2026	Initial release of IT Asset Disposal and Data Destruction Policy	President's Cabinet