Kingsborough Community College's restriction on external storage devices is directly aligned with CUNY cybersecurity standards governing data protection, access control, encryption, malware prevention, and auditability. The policy ensures institutional data remains within secured, monitored, and recoverable systems, reducing regulatory, operational, and reputational risk

Kingsborough Community College

Policy on the Use of External Storage Devices

1. Purpose

The purpose of this policy is to protect Kingsborough Community College (KCC) information assets from data loss, unauthorized disclosure, malware infection, and compliance violations by restricting the use of external storage devices on College-owned systems and within the campus environment.

---

2. Scope

This policy applies to:

- All faculty, staff, students, contractors, and affiliates
- All College-owned or College-managed computing devices
- All forms of removable or external storage, including but not limited to:
  - USB flash drives
  - External hard drives and SSDs
  - SD cards and memory cards
  - Portable media readers

---

3. Policy Statement

The use of external storage devices on College-owned systems is **prohibited by default** unless explicitly approved by the Office of Information Technology Services (OITS) for a documented business or academic need.

---

4. Rationale for Restriction

External storage devices present significant and well-documented risks to the College. These risks include, but are not limited to, the following:

4.1 Data Exfiltration and Loss

- External storage enables the rapid and undetectable copying of sensitive institutional data, including:
    - Student records (FERPA-protected)
    - Employee data
    - Research data
    - Financial and operational information
- Unlike centrally managed systems, data copied to external devices cannot be reliably tracked, audited, or revoked.

4.2 Inability to Enforce Data Protection Controls

- External devices fall outside the College's centralized security controls, including:
    - Encryption enforcement
    - Data Loss Prevention (DLP)
    - Access logging and monitoring
- The College cannot guarantee that data stored externally remains encrypted, intact, or accessed only by authorized individuals.

4.3 Physical Security Risks

- External storage devices are small, portable, and easily lost or stolen.
- The campus environment (shared offices, classrooms, labs, and public spaces) makes it impractical to ensure physical safeguarding of such devices.
- Loss of a single unencrypted device can result in a reportable data breach.

4.4 Lack of Reliable Backup and Recovery

- Data stored on external devices is typically:
    - Not included in College backup systems
    - Not protected by disaster recovery processes
- Loss, corruption, or failure of the device can result in permanent data loss with no recovery option.

4.5 Malware and Ransomware Introduction

- External storage devices are a common infection vector for:
    - Malware
    - Ransomware
    - Unauthorized or malicious software
- Devices introduced from home or external environments bypass many perimeter security controls.

4.6 Compliance and Regulatory Risk

- Use of unmanaged storage complicates compliance with:
    - FERPA
    - CUNY cybersecurity standards
    - State and federal data protection requirements
- In the event of an audit or incident, the College may be unable to demonstrate adequate safeguards or data handling practices.

4.7 Operational and Support Challenges

- External devices:
    - Increase troubleshooting complexity
    - Introduce compatibility and reliability issues
    - Divert IT resources from centrally supported, secure platforms
- They undermine standardized workflows built around secure network storage and cloud services.

---

5. Approved Alternatives

To meet legitimate academic and administrative needs, the College provides secure, supported alternatives, including:

- College-managed network storage
- Approved cloud storage platforms with access controls and audit logging
- Secure file-sharing solutions approved by OITS

These alternatives provide encryption, backup, access control, and compliance monitoring that external storage cannot reliably support.

---

6. Exceptions

Exceptions to this policy may be granted **only** when:

- There is a documented business or academic requirement that cannot be met through approved alternatives
- The device supports hardware encryption and meets OITS security standards
- Written approval is obtained from OITS

Approved exceptions may be time-limited and subject to additional controls.

---

7. Enforcement

- Unauthorized use of external storage devices may result in:
    - Device blocking or removal
    - Revocation of system access
    - Disciplinary action in accordance with College and CUNY policies
- OITS reserves the right to implement technical controls to enforce this policy.

---

8. Policy Review

This policy will be reviewed periodically to ensure alignment with evolving security threats, regulatory requirements, and institutional needs.

External Storage Device Policy

Alignment to CUNY Cybersecurity Standards

Institution: Kingsborough Community College
Governing Framework: City University of New York (CUNY) Cybersecurity Program

---

1. Governing CUNY Cybersecurity Frameworks Referenced

This policy aligns with the following CUNY-wide cybersecurity requirements and guidance:

- CUNY Cybersecurity Policy
- CUNY Information Security Standards
- CUNY Data Classification and Handling Guidelines
- CUNY Acceptable Use of Information Technology Resources Policy
- CUNY Incident Response and Breach Notification Requirements

These standards are collectively designed to protect **confidential, sensitive, and institutional data** across all CUNY campuses.

---

2. Control Mapping Summary

Policy Area	CUNY Control Domain	Alignment Explanation
Prohibition of unmanaged external storage	Access Control	Prevents unauthorized data movement and circumvention of access safeguards

Policy Area	CUNY Control Domain	Alignment Explanation
Data exfiltration prevention	Data Protection	Reduces risk of unauthorized disclosure of sensitive data
Encryption requirements	Cryptographic Controls	Ensures data at rest meets encryption standards
Malware risk mitigation	System & Network Security	Blocks common infection vectors
Physical security limitations	Asset Management	Addresses inability to secure portable assets
Backup and recovery limitations	Business Continuity & DR	Ensures data remains within supported backup systems
Exception management	Risk Management & Governance	Allows controlled, documented deviations

---

3. Detailed Standards Alignment

3.1 CUNY Data Classification & Handling

Relevant Requirement:
CUNY requires that sensitive and confidential data be stored, transmitted, and processed only on approved, secured systems.

Policy Alignment:

- External storage devices are unmanaged and cannot reliably enforce encryption, access controls, or audit logging.
- Prohibiting their use ensures sensitive data remains within College-controlled systems that meet classification requirements.

Risk Addressed:
Unauthorized disclosure of FERPA-protected and institutional data.

3.2 Access Control & Least Privilege

Relevant Requirement:
CUNY mandates access controls that restrict data to authorized users and approved systems.

Policy Alignment:

- External storage enables uncontrolled data replication outside authorized environments.
- Blocking such devices enforces least-privilege principles and prevents bypassing identity and access management controls.

Risk Addressed:
Loss of accountability and traceability for sensitive data.

3.3 Encryption & Cryptographic Standards

Relevant Requirement:
CUNY requires encryption of sensitive data at rest and in transit using approved methods.

Policy Alignment:

- The College cannot guarantee encryption on personally owned or unmanaged external devices.
- Approved exceptions require hardware-level encryption validated by OITS.

Risk Addressed:
Unencrypted data exposure resulting from device loss or theft.

3.4 Malware Prevention & Endpoint Security

Relevant Requirement:
CUNY cybersecurity standards require controls to prevent malware, ransomware, and unauthorized software introduction.

Policy Alignment:

- External storage is a known vector for malware propagation.
- Restricting removable media reduces exposure to threats that bypass perimeter defenses.

Risk Addressed:
Campus-wide compromise via infected removable media.

3.5 Asset Management & Physical Security

Relevant Requirement:
CUNY requires institutions to protect IT assets from loss, theft, and misuse.

Policy Alignment:

- Portable storage devices cannot be effectively inventoried, tracked, or physically secured in open campus environments.

- Prohibition eliminates unmanaged assets holding institutional data.

Risk Addressed:
Loss of sensitive data due to misplaced or stolen devices.

3.6 Backup, Retention & Disaster Recovery

Relevant Requirement:
CUNY mandates that institutional data be included in backup and recovery processes.

Policy Alignment:

- Data stored on external devices is excluded from centralized backup and DR systems.
- Restricting their use ensures data remains recoverable and protected.

Risk Addressed:
Permanent data loss and inability to restore critical information.

3.7 Incident Response & Audit Readiness

Relevant Requirement:
CUNY requires institutions to demonstrate control, traceability, and containment during security incidents.

Policy Alignment:

- External storage undermines audit trails and incident scoping.
- Policy enforcement ensures incidents can be investigated, contained, and reported accurately.

Risk Addressed:
Inability to determine breach scope or demonstrate due diligence.

---

4. Governance & Exception Control

CUNY Requirement:
Risk-based exceptions must be documented, approved, and periodically reviewed.

Policy Alignment:

- Exceptions require OITS approval, justification, encryption validation, and may be time-bound.
- Supports governance, accountability, and compliance oversight.

---

5. Compliance & Accreditation Relevance

This mapped policy supports:

- **Middle States (MSCHE)** Standard on Information Security and Institutional Effectiveness
- **CUNY Central cybersecurity compliance reviews**
- **State and federal audit expectations**
- **FERPA and privacy risk management**
