730.2 Data Classification and Handling Policy

Policy Title: Data Classification and Handling Policy
Policy Number: 730.2
Responsible Office: Information Technology Services
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: All employees, faculty, staff, students, student workers, contractors, vendors, and any individuals who handle or access institutional data in any form.
Alignment: FERPA; GLBA; recognized cybersecurity and data protection frameworks (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 the institutional framework for classifying and protecting data based on sensitivity, legal requirements, and risk. It defines handling requirements to ensure appropriate safeguards across College systems and supports regulatory compliance and institutional data security.

II. Scope

This policy applies to all institutional data, regardless of format or location, and to all systems, platforms, devices, and third-party services that store, process, transmit, or provide access to institutional data.

III. Definitions

Public Information — Information approved for public release without restriction.

Internal Information — Nonpublic institutional information intended for internal operational use.

Confidential Information — Information protected by law or institutional policy that could harm individuals or the College if improperly disclosed, including FERPA- and GLBA-protected data.

Restricted Information — Highly sensitive institutional data requiring the strictest safeguards due to legal, regulatory, or identity protection risk, including Social Security Numbers and authentication credentials.

Institutional Data — Any data created, received, processed, stored, or transmitted by NEMCC in support of its academic, administrative, operational, financial, or student services mission.

IV. Roles and Responsibilities

Data Owners — Functional leaders responsible for approving access and determining classification (e.g., Director of Admissions, Director of Human Resources, Vice President of Finance).

Data Stewards — Staff managing day-to-day data integrity, permissions, and workflows in systems such as Banner, Document Management, and LMS platforms.

Information Technology Services (ITS) — Implements controls, enforces technical safeguards, provides secure platforms, and monitors compliance.

V. Data Classification Categories

Institutional data is classified into four levels based on sensitivity, legal requirements, and potential institutional risk.

A. Public Information

Low Sensitivity: Information approved for public release.
Examples:

- Website content
- Course catalog
- Marketing materials
- Press releases
- Public policies
- Handling Requirements:
- No restrictions on distribution
- Must be accurate and official
- Store in College-approved platforms

B. Internal Information

Moderate Sensitivity: Non-public information intended for internal operational use.
Examples:

- Departmental procedures
- Meeting agendas
- Internal schedules
- Draft documents

Handling Requirements:

- Share only with authorized NEMCC personnel

- Store in SharePoint/OneDrive or departmental storage
- Do not post publicly

C. Confidential Information

High Sensitivity — FERPA/GLBA-protected: Information protected by law or policy that could harm individuals or NEMCC if improperly disclosed.

Examples:

- Student educational records (FERPA)
- Financial aid data (GLBA)
- Employee HR records
- Non-public financial or operational data
- Advising information
- Student discipline records

Handling Requirements:

- Access limited to individuals with a legitimate educational/administrative need
- Store only in approved systems (Banner, Document Management, secure cloud)
- DO NOT store on personal devices
- Email only to authorized recipients; never include SSNs
- Email containing Confidential data must use College-approved encryption
- Printed copies must be secured; shred when no longer needed
- Technical Controls:
- Least privilege (NIST AC-6)
- Logging of access (NIST AU-2)
- Encrypted storage where available (NIST SC-28)

D. Restricted Information

Maximum Sensitivity — SSN & Identity-Critical Data: —Information classified as Restricted Institutional Data requiring the strictest safeguards due to legal, regulatory, or identity protection risk.

Examples:

- Social Security Numbers (SSNs)
- Government-issued identification numbers
- Bank account and routing numbers
- Authentication credentials
- System API keys and tokens
- Data covered by the SSN Access Policy

Handling Requirements:

- Governed by the Social Security Number (SSN) Access and Protection Policy (730.1) and must follow its access-approval workflow
- DO NOT email, print, store on personal devices, or transmit through unencrypted methods
- Access only within approved encrypted systems (e.g., Banner, secure Document Management)
- Annual recertification required
- All access logged and subject to review
- Technical Controls:
- Access approval by Data Owner
- Encryption in transit/at rest (NIST SC-12, SC-28)
- Strict monitoring and alerting (NIST SI-4)
- No downloading or offline storage

VI. Handling Requirements Across All Data Levels

A. Storage

- Use only NEMCC-approved systems (SharePoint, OneDrive, Banner, Document Management, LMS)
- Personal USB drives or unencrypted external media are prohibited for Confidential or Restricted data

B. Transmission

- Use secure, College-managed services (encrypted email, Banner workflows, secure upload portals)
- Do not transmit Restricted data through email, chat, or standard file-sharing

C. Access Control

- Follow least-privilege principles

Access removed upon job change or separation in accordance with the Acceptable Use Policy (700.1) and the Account Lifecycle and Access Management Policy (700.5).

During safety, student conduct, or security investigations, an Account Suspension (AS) hold may be applied to preserve account state and protect Confidential or Restricted data in accordance with the Data Governance and Security Oversight Policy (735.0).

D. Printing & Physical Handling

Confidential or Restricted data must be secured immediately

Physical copies containing Confidential or Restricted institutional data must be placed in designated locked shredding containers serviced by an approved secure document destruction vendor. Disposal in regular trash or recycling receptacles is prohibited.

E. Disposal

All disposal of electronic or printed institutional data must comply with the IT Asset Disposal and Data Destruction Policy (770.1), including certified data sanitization, physical destruction for Restricted data, and required documentation.

VII. Third-Party Systems & Vendors

Before storing institutional data in a third-party system, ITS must assess the vendor for:

- Encryption capability
- Access logging
- FERPA/GLBA compliance
- Contractual security standards

Data Owners remain responsible for ensuring classification and appropriate handling.

VIII. Incident Reporting

Any suspected data exposure involving Confidential or Restricted Institutional Data must be reported immediately to Information Technology Services (ITS) for containment, documentation, and remediation.

IX. 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).

X. Exceptions

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

XI. 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 Data Classification and Handling Policy	President's Cabinet