700.1 Acceptable Use Policy

Policy Title: Acceptable Use Policy
Policy Number: 700.1
Responsible Office: Information Technology Services
Approval Authority: Administrative Council; President's Cabinet (Final Approval)
Applies To: All employees, faculty, staff, students, student workers, contractors, vendors, retirees, and any individuals who access College technology resources or institutional data
Alignment: FERPA; GLBA; ADA; Section 504; Section 508; recognized cybersecurity and privacy frameworks (as updated)
Effective Date: May 2026
Current Version: 1.0.0
Supersedes: Appropriate Computer Use Policy (August 2024)
Next Scheduled Review: January 2027

I. Policy Overview and Purpose

This policy establishes the standards governing appropriate and ethical use of College technology resources and institutional data. It defines user responsibilities, prohibited conduct, and security expectations to promote lawful, professional, and secure use of information systems and to support compliance with applicable legal and institutional requirements.

II. Scope

This policy applies to all College-owned or managed technology resources, including networks, devices, cloud services, enterprise systems, communication platforms, and any system used to access, process, or store institutional data.

III. Definitions

Key terms used in this policy, including Institutional Data, Confidential Information, Restricted Information, and governance roles, are defined in the Data Governance and Security Oversight Policy (735.0) and the Data Classification and Handling Policy (730.2).

IV. Behavioral Standards and Requirements

Users are expected to follow the behavioral, ethical, and professional standards defined in this section.

Users must:

- Lock screens or log out when away.
- Prevent unauthorized viewing of digital or printed institutional data.

- Secure printed materials and shred Confidential or Restricted documents.
- Access records only for legitimate institutional purposes.
- Use technology ethically and professionally.
- Respect privacy and intellectual property rights.
- Avoid misuse, harassment, or unauthorized activity.
- Protect systems, accounts, and institutional data.
- Understand they are responsible for all actions performed under their assigned accounts.
- Only access systems and institutional data for which they have authorization.

Requirements include:

- No credential sharing (including passphrases or passwords).
- No use of another person's credentials.
- No unauthorized access attempts.
- Unauthorized access includes any attempt to view, use, modify, copy, or disclose institutional data or systems without explicit approval.
- Report role or responsibility changes to ITS immediately.
- Student workers must follow the same requirements.

System protection requirements apply to the institutional Enterprise Resource Planning (ERP) system, learning management systems, reporting platforms, workflow and automation systems, document management systems, collaboration environments, administrative interfaces, and all current or future integrated institutional systems.

Disposal of digital or printed institutional data must follow the IT Asset Disposal and Data Destruction Policy (770.1). Secure destruction includes the use of secure shredding containers.

V. Standards for Email, Authentication, and Data Protection

A. Email and Communications

- Users must conduct all College-related communication using official NEMCC email accounts.
- Forwarding College email to any personal email account is prohibited.
- Email may be monitored for business, legal, or security purposes; no expectation of privacy exists.
- Email account creation, access duration, retention, suspension, and termination are governed by the Account Lifecycle and Access Management Policy (700.5). Sensitive, Confidential, or Restricted institutional data may not be forwarded, transmitted, or stored using email unless expressly approved and secured through College-managed systems.

B. Passwords, Passphrases, and Authentication

- Users must comply with the Authentication and Credential Security Policy (700.4). Requirements include:
- Use of passphrases (preferred) or passwords when required by legacy systems
- Use of Multi-Factor Authentication (MFA) wherever technically supported
- Never share authentication credentials
- Protect active sessions and avoid insecure storage of credentials
- Notify ITS immediately upon role change, suspected compromise, or termination

C. Information Classification and Data Restrictions

- Users must follow all data classification and handling requirements defined in the Data Classification and Handling Policy (730.2).
- Restrictions include:
- Institutional data may only be accessed for legitimate institutional purposes
- Printed institutional data must be protected and securely shredded when no longer needed

Confidential Institutional Data, as defined in Policy 730.2, may be emailed only when protected with College-approved encryption (e.g., Microsoft Purview Message Encryption or S/MIME) and appropriate sensitivity labels, and only to authorized recipients. Restricted data must not be emailed and may only be accessed via approved encrypted institutional systems and workflows.

Users are responsible for protecting institutional data in any form—digital or printed—and must immediately report any suspected exposure or unauthorized access to ITS.

VI. Appropriate Use and Copyright Requirements

Users must use College technology resources, systems, networks, accounts, and institutional data only for legitimate institutional purposes. Permitted uses include instructional activities, official College business, research, study, and the use of approved systems.

Prohibited uses include:

- Commercial or financial gain unrelated to College business.
- Partisan political activity.
- Harassment, intimidation, or abusive behavior.
- Accessing, creating, or distributing pornographic or obscene material.
- Circumventing or attempting to bypass security controls.
- Installing or using unauthorized software.
- Scanning for vulnerabilities without authorization.
- Misrepresenting personal views as official College positions.
- Excessive consumption of technology resources.

Users must comply with all copyright, intellectual property, and licensing requirements. Unauthorized downloading, distribution, or sharing of copyrighted materials—including through peer-to-peer services—is prohibited. Peer-to-peer traffic may be blocked. Repeat offenders may face disciplinary action.

VII. Special Compliance Requirements

A. Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) tools may be used to support instruction and administrative operations only when such use complies with all applicable institutional policies, including the Data Classification and Handling Policy (730.2), the Data Governance and Security Oversight Policy (735.0), and all security, privacy, accessibility, and academic integrity requirements.

Users must not upload, process, store, or transmit Confidential or Restricted institutional data in AI systems unless the system has been formally reviewed and authorized by Information Technology Services (ITS) and the appropriate Data Owner in accordance with institutional governance procedures.

AI systems must not be used in a manner that violates FERPA, GLBA, accessibility requirements, copyright law, or institutional conduct standards.

Users are responsible for reviewing and validating AI-generated content for accuracy, reliability, bias, security implications, and compliance before use, publication, or distribution.

The College does not endorse, certify, or recommend specific AI tools.

B. Accessibility Standards

All technology use must comply with applicable accessibility requirements, including:

- The Americans with Disabilities Act (ADA)
- Section 504 of the Rehabilitation Act
- Section 508 of the Rehabilitation Act
- WCAG 2.1 AA
- WCAG2ICT

Users must ensure that all digital content they create, post, share, or distribute—including documents, presentations, instructional materials, communication content, and media—meets required accessibility standards. Users must cooperate with ITS, Instruction, or Distance Education when accessibility remediation is required.

All digital content and technology use must meet accessibility requirements defined in the Technology Accessibility Policy (760.1), including WCAG 2.1 AA, ADA, Section 504, Section 508, and WCAG2ICT standards. Accessibility-related exceptions must follow the EAAAP process in Policy 760.1.

VIII. 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).

IX. Exceptions

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

X. 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 updated Acceptable Use Policy. Supersedes the "Appropriate Computer Use Policy" (Aug 2024)	President's Cabinet