Policy:
Artificial Intelligence (AI) and Data Usage

Contents

1.0 Policy Statement 2
2.0 Policy Scope 2
3.0 Policy 3
4.0 Official Le Moyne AI Tools & Security Standards 3
5.0 Data Privacy and Security 4
a. Administrative Visibility and eDiscovery (Internal Privacy) 4
b. Prohibited Submissions (Public AI Tools) 4
c. Third-Party Copyright and Library Database Terms 5
d. Third-Party & Non-Enterprise Tools 6
e. Incident Reporting 6
f. Protection of Student Intellectual Property and Coursework: 6
6.0 AI Data Governance & Authority 6
7.0 Instructional Autonomy and Academic Integrity 7
a. Instructor Authority 7
b. Syllabus Requirements 7
c. Assessment Integrity & Inclusivity 7
8.0 Research, Authorship, and Verification 8
a. Authorship and Attribution: 8
b. Verification and "Hallucinations": 8
c. Academic and Professional Misconduct: 8
d. Sponsored Programs and IRB Compliance: 9
9.0 Ethical Labor Practices & Operational Innovation 9
10.0 Prohibited Conduct 9
11.0 Reporting Inappropriate Use of AI 9
12.0 Definitions 10
13.0 References and Related Policies and Procedures 10
14.0 Policy History 11

1.0 PREAMBLE

Le Moyne College prioritizes academic excellence in the Catholic and Jesuit tradition and emphasizes educating the whole person and promoting the search for meaning and value as integral parts of the intellectual life. Given Le Moyne College's commitment to intellectual integrity, critical inquiry, and personal development, the following Artificial Intelligence (AI) policy establishes a framework for a more conscientious response to these technologies—a student-focused response that acknowledges that AI can be intentionally used or not used to enhance learning, build character, support scholarly and creative work, and advance institutional effectiveness. Grounded in our dedication to nuanced, imperfect, and authentically human relationships; our prioritization of learning environments built on academic honesty and trust; our care for our immediate and our global communities; and our obligation to protect institutional data and support individual wellbeing, this policy affirms that, at its best, AI can be a tool to support—not replace—human learning, judgment, creativity, and accountability. Guided by our goal to empower the College community to respond to AI as critically, ethically, and responsibly as possible, we affirm that, within this landscape of constant change and development, Le Moyne College is committed to developing students who reflect, reason, and lead with virtue and compassion.

2.0 POLICY STATEMENT

To uphold the values articulated above, Le Moyne College establishes this policy to govern the thoughtful, ethical, and secure integration of Artificial Intelligence (AI) across the institution. This framework ensures that AI technologies are adopted in a manner that preserves intellectual integrity, protects institutional security, and empowers the College community to engage with emerging technologies critically and responsibly.

3.0 POLICY SCOPE

This policy applies to all members of the Le Moyne community, including faculty, staff, students, and affiliates. It governs the use of AI technologies—including generative, traditional, and agentic AI—for all college-affiliated business, instruction, and research, whether conducted on or off campus.

4.0 POLICY

Guiding Principles

Le Moyne College embraces Artificial Intelligence as a tool to amplify human potential, anchored by our Jesuit values and a commitment to "Greatness meets Goodness." Our adoption of AI is guided by seven core pillars:

1. Human-Centered Responsibility: AI is a collaborator, not a replacement for human judgment, mentorship, or care. Individuals remain 100% responsible for all content produced with AI assistance. AI output must be treated as a draft until it is reviewed, validated, and approved by a human.
2. Mission Alignment: AI use must support the College's mission of advancing learning through the integration of teaching, research, and service. We use these tools to turn information into wisdom, preparing our community for leadership and service in a modern society.
3. Responsible Innovation: In the spirit of adapting to the "needs of the times," we encourage experimentation to enhance creativity and efficiency. However, the impact of AI on educational outcomes and institutional integrity must be rigorously and continuously assessed.
4. Equity and Access: To prevent a "cognitive divide," AI adoption must not disadvantage students based on their ability to access paid or premium technologies. The College provides enterprise-level tools to all members to ensure a level playing field.
5. Secure Sovereignty & Contextual Transparency: We prioritize the security of our community's data and honesty in our work.
6. Data Sovereignty: All work involving non-public institutional data must remain within Le Moyne's enterprise environment.
7. Contextual Transparency: Disclosure of AI assistance is required for substantive academic, scholarly, or public-facing institutional work (e.g., grant proposals, accreditation reports, public statements). It is not required for routine administrative productivity tasks (e.g., drafting internal emails, creating meeting agendas, or formatting spreadsheets).

5.0 OFFICIAL LE MOYNE AI TOOLS & SECURITY STANDARDS

To ensure a secure digital environment that protects our community's intellectual property, the College maintains a Protected Institutional Environment approach to AI.

- Designated Tools: Google Gemini and Google NotebookLM are established as the official AI tools for Le Moyne-affiliated work.
- Secure Access Requirement: Community members must access AI tools exclusively through their Le Moyne-issued accounts whenever they are performing Le Moyne work, handling institutional data, or utilizing a College-owned device.
- The Protected Standard: Accessing Gemini through an enterprise account ensures that all submitted prompts and data are walled off from the public internet. Unlike free/public versions of AI, this Protected Institutional Environment prevents submitted information from being used to train external models.

- Business & Research Requirement: All official College business, administrative tasks, and research involving non-public data must be conducted within these licensed environments to mitigate institutional risk and ensure data sovereignty.
- Accessibility Standard: All institutionally supported AI tools meet WCAG 2.1 AA accessibility standards.
- Evolving Toolkit: As AI technologies continue to develop, the CIO—working with academic, administrative, and governance partners—may approve additional enterprise-grade AI tools that uphold Le Moyne's commitments to data sovereignty, accessibility, equity, and responsible innovation. Newly approved tools will be added to the Official Le Moyne Toolkit without requiring a formal policy rewrite.

6.0 Data Privacy and Security

Protecting institutional, research, and personal data is a mandatory requirement for all AI interactions. Our security posture relies on maintaining a clear boundary between our Protected Institutional Environment and the public web.

a. Administrative Visibility and eDiscovery (Internal Privacy)

Le Moyne College provides a Protected Institutional Environment (e.g., Enterprise Gemini) to ensure our data is not used to train public AI models. This environment is designed to protect our community from external data harvesting, *not* to serve as an internal surveillance tool.

- Routine Monitoring: Information & Technology Services (IT) does not routinely monitor, read, or audit the content of individual AI prompts or generated responses.
- Academic Integrity Requests: IT will not fulfill ad-hoc requests from faculty to search a student's AI prompt history to investigate suspected academic dishonesty. Faculty must rely on the holistic academic judgment and assessment standards outlined in Section 5 of this policy.
- Authorized Access: Because Gemini is an enterprise system, interaction logs are technically retained by Google Vault for legal compliance. However, these logs will only be accessed or exported by IT during a formal cybersecurity investigation, a legal subpoena, or an official institutional inquiry explicitly authorized by the Provost, Human Resources, or the Office of the President.

b. Prohibited Submissions (Public AI Tools)

Users are **strictly prohibited** from inputting the following data tiers into publicly available or consumer-tier AI tools (e.g., personal ChatGPT, Claude, or non-Le Moyne Gemini accounts). These data types must stay within Le Moyne's Enterprise environment or, in the case of Restricted data, remain out of AI systems entirely:

- Restricted (Level 4) Data – NEVER PERMITTED:
    - PII & Financial Data: Social Security Numbers, bank account/wire transfer info, or government-issued IDs.
    - Protected Health Information (PHI): Any health-related data covered under HIPAA.

    - High-Stakes Student Records: Financial aid records (GLBA), disability accommodations, or disciplinary files.
    - Authentication & IT Security Data: Computer/system passwords, database credentials, API keys, or network security configurations.

- Private (Level 3) Data – ENTERPRISE ONLY + AIIA REQUIRED:
    - FERPA-Protected Records: Student grades, transcripts, and class schedules.
    - Institutional Property: Non-public building plans, legal billings, contract negotiations, or donor lists.
    - Personnel Data: Employee home addresses, personal phone numbers, or beneficiary info.

- Internal (Level 2) Data – ENTERPRISE STRONGLY PREFERRED:
    - Operational & Academic Materials: Internal department budgets, committee minutes, draft syllabi, course assignments, grading rubrics, and internal memos. While lower risk, use of consumer AI for L2 data is highly discouraged to prevent accidental "data seepage" into public models.

Handling Mixed Data: It is common for documents to contain multiple tiers of data (e.g., a standard Level 3 transcript that includes a Level 4 disciplinary notation). If a document or prompt contains mixed data classifications, users must always apply the security controls of the **highest** data tier present. When in doubt about whether a student record is routine (Level 3) or high-stakes (Level 4), users must default to Level 4 protections or consult the official Data Owners (e.g., Registrar, Dean of Students) before using AI.

c. Third-Party Copyright and Library Database Terms

While Le Moyne College provides a Protected Institutional Environment for AI use, users must strictly adhere to the Terms of Service, End-User License Agreements (EULAs), and copyright restrictions of third-party vendors, publishers, and library databases.

- Vendor Rules Supersede: If a publisher or database explicitly prohibits the uploading, scraping, or processing of their licensed content into Artificial Intelligence tools, users must comply with that restriction—even when using Le Moyne's protected Gemini or NotebookLM environments.
- User Responsibility: The College's provision of secure AI tools does not override external copyright law or vendor contracts. It is the individual user's responsibility to verify the AI-use permissions of external datasets, academic articles, or proprietary research platforms before importing that data into an AI model.
- Intellectual Property and Peer Materials: Faculty and staff may not upload course materials, rubrics, research data, or syllabi authored by colleagues into any AI system—including Le Moyne's protected enterprise environments—without explicit permission from the original author. While using the College's secure AI prevents external data scraping, uploading a colleague's work into a public/consumer-tier AI tool carries the additional severity of constituting an unauthorized release of institutional data.

d. Third-Party & Non-Enterprise Tools

Since the AI marketplace is expanding rapidly, users must exercise extreme caution with non-enterprise subscription models and third-party browser extensions.

The Training Risk: Unless an official Le Moyne contract is in place, users must assume that any data entered into a non-enterprise tool becomes part of a public training set and is no longer private or protected.

Non-Vetted Status: Use of AI tools outside of the Official Le Moyne Toolkit (Section 2) for institutional business is conducted at the user's own risk. Violations resulting in data exposure will be referred to the appropriate disciplinary body (e.g., Human Resources for staff, the Provost's Office for faculty, or the Student Conduct process for students).

e. Incident Reporting

Any potential or actual breach of data confidentiality—such as the accidental input of sensitive records into a public AI tool—must be reported immediately to the IT Security Team**.** Early reporting is critical to mitigating institutional risk and fulfilling our legal notification obligations. These reports will be triaged and classified in accordance with the *IT Procedure: AI Implementation & Incident Response*.

f. Protection of Student Intellectual Property and Coursework:

Student assignments, essays, exams, and projects are the intellectual property of the student and constitute FERPA-protected educational records.

- Public AI Tools Prohibited: Faculty and staff are strictly prohibited from uploading student coursework into public or consumer-tier AI tools (including public AI-detection websites or free ChatGPT) for any reason, including grading, feedback, or AI-detection, without explicit, written consent from the student.
- Enterprise Tools for Grading: Faculty may use Le Moyne's Protected Institutional Environment (e.g., Enterprise Gemini) to assist with rubric alignment or generating feedback on student work, provided the student's personally identifiable information (PII) is removed from the prompt. However, faculty retain 100% responsibility for the final grade and feedback provided.

7.0 AI Data Governance & Authority

This policy operates in conjunction with the *Le Moyne Data Classification Policy*. To ensure institutional security and data sovereignty, the following specific authorities apply to all AI-related activities:

- Data Owners (Deans, Department Heads, VPs): Responsible for identifying the classification tier of data within their domain and requesting its use within specific AI tools. A Data Owner's approval signifies a functional or academic "Yes" but does not constitute final technical authorization.

- Data Custodians (IT/CIO): Responsible for vetting the security, privacy, and technical architecture of AI environments. The CIO (or designee) maintains final "Gatekeeper" authority. IT may veto, deny, or suspend the use of any AI tool—regardless of Data Owner approval—if the tool or workflow presents an unacceptable risk to the College's data security or legal compliance.
- Data Users (Faculty, Staff, Affiliates): Responsible for handling data strictly in accordance with its classification. Users are strictly prohibited from using personal or non-enterprise AI accounts when processing non-public (Internal, Private, or Restricted) Le Moyne data.

8.0 Instructional Autonomy and Academic Integrity

Pedagogical use of AI is decentralized; faculty maintain primary authority over their classroom environment and the integration of AI tools into their curricula.

a. Instructor Authority

Faculty define the role of AI in their specific courses. In the absence of explicit permission in a syllabus or assignment instructions, the use of AI to complete academic work is considered a violation of the Student Code of Conduct. It is the student's responsibility to clarify AI expectations with their instructor before submission.

b. Syllabus Requirements

To provide clarity and ensure the Equity and Access of all students, each syllabus must categorize AI use under one of the following levels. If use is permitted, students should be directed to use Le Moyne's Protected Institutional Environment.

- AI Prohibited: AI tools may not be used for any portion of assignments or exams. All work must be the student's original intellectual product.
- AI Limited: AI is permitted only for specific, defined tasks (e.g., brainstorming, grammar support, or refining research questions) or assignments. Students must disclose the nature of AI assistance upon submission.
- AI Integrated: AI use is permitted or required as a core part of the learning process. Students may use AI for drafting, analyzing, or creating output while maintaining human oversight.

c. Assessment Integrity & Inclusivity

- Authentic Assessment: Faculty are encouraged to utilize "authentic assessment" methods—such as oral exams, in-class writing, or iterative project stages—that prioritize the learning process over the final output.
- Alternative Pathways: In alignment with our Human-Centered principle, faculty should consider providing alternative pathways for students who choose not to engage with AI for ethical or pedagogical reasons.
- Verification Authority: While AI detection software is inconsistent, faculty reserve the right to question students on their work and process to ensure human-centered responsibility. However, AI-detection scores (e.g., Turnitin AI percentages) or unverified hunches may not

be used as the sole basis for an academic penalty or a failing grade. Any disciplinary action must follow the standard outlined in the Academic Standards Policies within the Student Handbook.

9.0 Research, Authorship, and Verification

Human accountability is the non-negotiable standard for all professional, administrative, and scholarly output at Le Moyne College.

a. Authorship and Attribution:

- Authorship Eligibility: AI systems lack legal and ethical standing and therefore cannot be listed as authors or co-authors on any college-affiliated research, publications, or formal reports.
- Citation and Disclosure Standards: All AI assistance must be transparently cited according to discipline-specific standards (e.g., APA, MLA, or Chicago). This includes identifying the tool name, the version (e.g., Gemini (Enterprise Version)), and the specific nature of its contribution to the work.

b. Verification and "Hallucinations":

- Human Review Standard: Users must treat all AI-generated output as a draft that requires rigorous human review. AI models are known to produce "hallucinations"—plausible-sounding but factually incorrect information, including fabricated citations and data.
- Bias and DEI Accountability: Users should be aware that AI models may reflect societal biases present in their training data. It is the user's responsibility to ensure that final outputs align with Le Moyne's commitment to diversity, equity, and inclusion.
- Professional Verification: AI may only supplement—not replace—traditional methods of peer review or faculty evaluation and must be independently verified to ensure accuracy, fairness, and the integrity of the scholarly process.

c. Academic and Professional Misconduct:

- Defining Misconduct: Submitting AI-generated content as one's own original work, or using AI to fabricate research data, citations, or case studies, constitutes academic/professional misconduct.
- Detection and Judgement: The College does not rely solely on AI detection software, which can produce false positives and negatives. Instead, Le Moyne relies on holistic academic judgment—evaluating the consistency, depth, and unique voice of the student's or staff member's work over time.
- Administrative Accountability: For staff and administrators, the use of AI to generate official college correspondence or records must still meet the standard of Human-in-the-Loop verification to ensure institutional accuracy and brand alignment.

d. Sponsored Programs and IRB Compliance:

- AI use in externally funded research must strictly comply with sponsor requirements, export control laws, and Institutional Review Board (IRB) standards. Researchers are responsible for verifying that AI tool usage does not violate sponsor data-use agreements. For research involving human subjects, AI-assisted data analysis must be explicitly disclosed in IRB submissions.

10.0 Ethical Labor Practices & Operational Innovation

Consistent with our commitment to human-centered relationships, any decision to integrate AI into administrative or operational workflows will be guided by the following:

- Ethical Impact Assessment: Before adopting AI tools that significantly automate staff responsibilities, departments must complete a formal AI Impact Assessment as outlined in the IT Procedure: AI Implementation & Incident Response.
- Transparency and Feedback: Employees will be informed of the rationale for AI adoption and given opportunities to provide feedback throughout the decision-making process.
- Equitable Benefit Distribution: The College will strive to ensure that the benefits of AI (such as efficiency gains) are distributed equitably and do not create a "cognitive divide" or disproportionately disadvantage any group.

11.0 Prohibited Conduct

To maintain a safe and ethical environment, the following uses of AI are strictly prohibited for all members of the Le Moyne community:

- Harmful Content Generation: Using AI tools to intentionally generate content that constitutes discrimination, sexual harassment, stalking, or sexual exploitation.
- Facilitation of Illegal Acts: Using AI to generate content, instructions, or code that facilitates the violation of federal, state, or local laws.
- Systemic and Policy Violations: Using AI to intentionally circumvent College security protocols or violate existing institutional rules and guidelines.
- Automated Decision-Making: Using AI as the sole determining authority in high-impact institutional decisions—including admissions, hiring, promotion, tenure, financial aid allocation, student discipline, or employee termination. A human must always make the final determination in these matters.

12.0 Reporting Inappropriate Use of AI

To ensure that all members of the College community can raise concerns regarding the ethical or unauthorized use of AI, the following reporting pathways are established:

- Student Misuse: Suspected unauthorized use of AI in coursework or violations of ethical standards in academic matters should be handled according to the procedures outlined in the Academic Standards Policy or by contacting the appropriate academic dean.
- Faculty Misuse: If a faculty member is suspected of inappropriately using AI in their professional duties (such as in peer review or grading), the issue should be reported to the Provost.
- Research Misuse: Any suspected ethical violations involving AI in research or scholarship should be reported directly to the Institutional Review Board (IRB) or the Office of Research.
- Staff Misuse: Suspected misuse of AI by staff or administrators in official college business should be reported to the immediate supervisor or to Human Resources.
- Data Security Incidents: As previously noted, any accidental input of sensitive or restricted institutional records into a public AI tool must be reported immediately to the IT Security Team.

13.0 Definitions

- Agentic AI: AI systems designed to act autonomously or semi-autonomously to execute workflows, use software tools, or make decisions to achieve a specific goal with minimal human prompting.
- AI Hallucination: Confidently generated false information or fabricated citations.
- Generative AI: AI tools capable of creating new content (text, images, audio, or code).
- Human-in-the-Loop: The mandatory process of a human reviewing and approving AI-generated drafts before they are used or submitted.
- Institutional Data: Any data related to college operations, including restricted or critical records (FERPA, PII, Financial).
- Protected Institutional Environment: The secure Le Moyne-licensed instance where data is shielded from public training sets.
- Traditional AI: Systems used for data analysis, prediction, or automation (e.g., predictive analytics in enrollment).

14.0 References and Related Policies and Procedures

- IT Procedure: Artificial Intelligence Implementation & Incident Response (Companion Document)
- Acceptable Use Policy
- Data Classification Policy
- Cybersecurity Incident Response Plan
- Student Conduct Process
- Academic Standards Policy
- Computer Use Policy
- Faculty Handbook
- Employee Handbook

- FERPA Policy
- PHI/HIPAA Policy
- Institutional Review Board (IRB) Guidelines
- IT Procurement / Purchasing Policy

15.0 POLICY HISTORY

Version	Date	Author	Revisions
1.00	6/10/2026	Le Moyne College	Original

Periodic Review Mechanism: To ensure this policy remains responsive to the evolving digital landscape, the AI Governance Committee that meets quarterly and oversees tool approval, incidents, training, and policy updates. This group will be charged with reviewing technological advancements, assessing institutional impact, and updating these guidelines to reflect current ethical and educational standards.