LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

| SUBJECT: | Effective Date: | Policy Number: |
|---|---|---|
| Artificial Intelligence (AI) Policy | September 2024 | 05-1-015 |
| | **Supersedes:**<br>Policy:<br>Date: | **Page 1 Of 4** |
| | **Responsible Authority:** VP of IT & CIO | |

## I. Purpose and statement of operational policy underlying the procedure.

The purpose of this Artificial Intelligence (AI) Policy is to establish guidelines for the ethical and responsible use of AI technologies at LeMoyne-Owen College. This policy ensures that AI is used to enhance learning, research, operations, and services while protecting the privacy, security, and rights of students, faculty, staff, and other stakeholders.

## II. Applicability/Scope

This policy applies to all faculty, staff, students, contractors, and third-party vendors who use AI technologies within LeMoyne-Owen College's systems, services, and operations. It covers the development, implementation, and use of AI tools in academic, administrative, and operational activities.

**Definitions**

- **Artificial Intelligence (AI):** AI refers to systems or machines that mimic human intelligence to perform tasks such as learning, decision-making, problem-solving, and data analysis.
- **Machine Learning (ML):** A subset of AI that enables systems to learn and improve from experience without being explicitly programmed.
- **Data Privacy:** The protection of personal information from unauthorized access and use, ensuring confidentiality and compliance with legal obligations.
- **Bias in AI:** Systematic errors or prejudices in AI outputs due to flawed data, models, or algorithms, leading to unfair or discriminatory outcomes.

**Guiding Principles for AI Use**

- **Ethical Use:** AI technologies at LeMoyne-Owen College must be used ethically, with a focus on fairness, transparency, and accountability.
- **Transparency:** The development and deployment of AI systems must be transparent, providing clear explanations of how decisions are made and the role of AI in those decisions.
- **Data Privacy and Security:** AI systems must adhere to strict data privacy and security standards. Personal and sensitive data used in AI processes must be protected in accordance with the college's Data Management Policy and applicable laws.
- **Human Oversight:** AI systems should complement human decision-making, not replace it. Final decisions with significant academic or operational impact must include human oversight to ensure fairness and accountability.
- **Bias Mitigation:** AI systems must be regularly evaluated to detect and mitigate bias or discrimination in their outputs, ensuring equitable outcomes for all individuals and groups.

**Use of AI in Academic and Research Settings**

- **Academic Integrity:** Faculty and students must use AI tools in a manner that upholds the college's academic integrity standards. Plagiarism, cheating, or using AI to generate work without proper attribution or authorization is strictly prohibited.
- **AI in Instruction:** AI may be used as a teaching aid to enhance learning experiences. Faculty must ensure that AI tools are appropriately integrated into curricula, and students must be informed when AI is being used in the classroom.
- **Research Ethics:** Researchers using AI in their projects must comply with ethical standards for research, including protecting participant privacy and ensuring the integrity of the research process.

**Use of AI in Administrative and Operational Settings**

- **Automation of Services:** AI technologies may be used to improve the efficiency of college operations, including administrative processes, student services, and IT functions. However, AI-driven automation must not replace essential human interactions and decision-making in areas such as academic advising, financial aid, and student support.
- **AI in Decision-Making:** When AI is used to assist in decision-making processes (e.g., admissions, financial aid allocation), it must be designed and tested to ensure fairness, transparency, and the elimination of bias. Decisions affecting individuals must be reviewed and approved by authorized personnel.
- **Monitoring and Evaluation:** The college will regularly evaluate the performance of AI systems in administrative and operational activities to ensure they are operating as intended and in compliance with this policy.

**Data Privacy and Security in AI**

- **Data Collection and Use:** Any data used by AI systems must be collected and processed in accordance with LeMoyne-Owen College's Data Management Policy and applicable privacy

laws, including the Family Educational Rights and Privacy Act (FERPA) and General Data Protection Regulation (GDPR), where applicable.

- **Informed Consent:** Where applicable, students, faculty, and staff must be informed when their data is used in AI systems and provide consent for the use of their personal information.
- **Security Controls:** AI systems must be secured using encryption, access control, and other protective measures to safeguard sensitive information and prevent unauthorized access.

**Training and Awareness**

- **Training for AI Users:** Faculty, staff, and students who engage with AI tools and systems must receive training on how to use these technologies responsibly and ethically. Training resources will be provided by the IT Department or other relevant offices.
- **Raising Awareness:** The college will promote awareness of AI's potential benefits and risks, providing guidelines and resources on how to evaluate and use AI systems effectively in both academic and operational contexts.

**Compliance and Enforcement**

- **Compliance Monitoring:** The Office of Information Technology, in collaboration with other departments, will monitor the use of AI systems to ensure compliance with this policy.
- **Non-Compliance:** Violations of this policy may result in disciplinary action, including but not limited to revocation of AI usage privileges, termination of employment, or expulsion for students, depending on the severity of the violation.
- **Reporting Violations:** Any concerns or violations of this policy should be reported to the IT Department or Human Resources for investigation.

## III. Process for Implementing Procedure

| Responsibility | Action | Timeline |
|---|---|---|
| IT Department | Responsible for implementing and managing access controls, conducting audits, and responding to security incidents. | Ongoing |
| Department Heads | Approve access requests for their team members and ensure access is appropriate for the individual's role. | Ongoing |
| Users | Responsible for complying with access control policies, safeguarding credentials, and reporting suspicious activity. | Ongoing |
| Authorizing Official | This Access Control Policy will be reviewed annually and updated as necessary to reflect changes in technology, risks, | Annually |

| | | |
|---|---|---|
| | and regulatory requirements. | |

## IV. Related policies/References for more information

- Acceptable Use Policy
- Data Management Policy

Authorizing Official: _____ Authorization Date: _____

Title: _ _____