Jamestown Community College
Policies and Procedures

Policy Title	**Artificial Intelligence (AI)**	**Policy Number**	**010**
Section	**Governance, Organization and General Information**	**Approval Date**	**10/21/2025**
Subsection	**Governance and Organization**	**Effective Date**	**10/21/2025**
Responsible Office	**Planning**	**Review Date**	

1.0 Purpose

This policy establishes the principles and responsibilities for the use of Artificial Intelligence (AI) across all operations of Jamestown Community College, ensuring alignment with the institution's mission, commitment to student success, ethical standards, and accreditation requirements defined by the Middle States Commission on Higher Education.

Jamestown Community College continues to advance its vision "to support our students' journey to success in the local and global workplace with quality, in-demand learning experiences" by embracing the use of technology, including AI, to best prepare our students for career success. In addition, JCC recognizes the importance of AI in streamlining administrative processes and improving efficiency.

The development of a Jamestown Community College AI Position Statement in early 2025 set the stage for AI integration while recognizing the safeguards that are required for the safe and ethical use of AI. The following AI use policy and accompanying procedures, guidelines, and principles further JCC's resolve to embrace AI lawfully, ethically, safely, securely, and transparently. This policy also supports compliance with MSCHE's Use of Artificial Intelligence Policy and Procedures, which took effect on July 1, 2025.

2.0 Policy

All Jamestown Community College community members (students, employees, and those performing work or services for the college) who use AI for college purposes shall do so lawfully, ethically, safely, securely, and transparently.

Lawful Use of AI: AI use must comply with all applicable institutional policies, federal and state laws, accreditation standards, and contractual obligations.

Ethical Use of AI: Human oversight is required for all AI-generated content to ensure accuracy, reliability, and freedom from bias. Fully automated decision-making without meaningful human

involvement is prohibited. Any AI intended for use in decision-making processes must be reviewed and approved by the College's Information Security Committee.

Safe and Secure Use of AI: The use of protected information or personally identifiable information (PII) with AI tools is prohibited unless the tool has been formally approved by the college's Information Security Committee.

Transparent Use of AI: All uses of AI, including for creating written or academic work, must be disclosed. AI use in institutional assessment, analytics, or decision-making processes must be transparent and traceable.

3.0 Procedures

4.0 Definitions

Artificial Intelligence (AI): systems or tools that perform tasks typically requiring human intelligence, such as generating text, analyzing data, or making recommendations

Generative AI: a subset of AI that uses generative models to create content, including text, images, audio, or code

Automated Decision-Making: Use of AI to support or replace human decision-making processes

Confidential Information: Information that is strictly protected by law, regulation, contract, or institutional policy due to its sensitivity. Unauthorized disclosure could result in legal liability, identity theft, financial loss, or institutional risk. Examples include, but are not limited to:

- Social Security numbers
- Credit card or bank account numbers
- Driver's license numbers
- Protected student records (FERPA)
- Employment records (e.g., disciplinary files, benefits information)
- Medical or health-related information (e.g., disability accommodations, mental health data)
- College financial records not publicly disclosed
- Credentials (e.g., passwords, private keys)

Sensitive Information: Information that is not legally regulated to the same degree as Confidential Information but still requires protection due to ethical, privacy, or operational concerns. Its unauthorized disclosure may cause embarrassment, reputational harm, or disruption. Examples include, but are not limited to:

- Full names in combination with contact information (address, phone number, email)
- ID numbers (e.g., student ID, employee ID) when not tied to sensitive data
- Class rosters
- Internal planning documents
- Research data not yet published

Personally Identifiable Information (PII): Any information that can be used to distinguish or trace an individual's identity, such as name, ID number, date of birth, or biometric records, alone or when combined with other personal or identifying data.

Protected Information: A general term referring to both Confidential and Sensitive Information. It is not intended for public disclosure and must be handled according to applicable laws and policies.

5.0 References

AI Use in Teaching and Learning: Principles and Guidelines for Faculty

AI Use in Teaching and Learning: Principles and Guidelines for Students

AI Use in Administrative Work: Principles and Guidelines for Employees

Jamestown Community College procurement procedures

Student Constitution – Academic Integrity

6.0 Guidance Documents