BROOKDALE COMMUNITY COLLEGE
COLLEGE REGULATION

2.9005R Artificial Intelligence Governance and Responsible Use Regulation

I. Title of Regulation

2.9005R Artificial Intelligence Governance and Responsible Use Regulation

II. Objective of Regulation

The purpose of this Regulation is to establish standards governing the responsible acquisition, implementation, and use of Artificial Intelligence (AI) technologies throughout Brookdale Community College.

The College recognizes AI as a valuable tool for enhancing teaching, learning, student success, research, institutional effectiveness, and administrative operations. At the same time, AI must be used responsibly, ethically, transparently, securely, and in compliance with applicable laws, accreditation standards, and College policies.

AI is intended to augment—not replace—human judgment, professional expertise, or institutional decision-making.

III. Authority

This Regulation is promulgated pursuant to the College's Artificial Intelligence Governance and Responsible Use Policy.

This Regulation is intended to support the College's mission and comply with applicable federal and State of New Jersey laws, accreditation requirements of the Middle States Commission on Higher Education (MSCHE), and all other applicable College policies relating to information technology, academic integrity, records management, privacy, accessibility, procurement, and cybersecurity.

IV. Regulation Statement

This Regulation applies to:

- Trustees
- Faculty
- Staff
- Administrators
- Students
- Contractors

- Consultants
- Vendors providing AI-enabled services
- Any individual using AI technologies on behalf of the College or utilizing College information or systems

Definitions

For purposes of this Regulation:

Artificial Intelligence (AI) refers to software systems that perform tasks requiring human-like reasoning, learning, prediction, classification, content generation, or decision support through machine learning, automation, statistical modeling, natural language processing, or similar technologies.

Generative AI refers to AI capable of producing new text, images, audio, video, software code, or other content based upon user prompts.

Predictive AI refers to AI systems that analyze data to forecast future outcomes or trends.

Agentic AI refers to autonomous AI systems capable of independently planning and executing multi-step tasks toward defined objectives.

Large Language Model (LLM) refers to an AI model trained on large collections of text capable of understanding and generating human language.

Artificial Intelligence System means any software platform or application utilizing AI technologies.

Personally Identifiable Information (PII) means information that can identify an individual as defined by applicable federal or state law.

Confidential Information includes institutional, financial, personnel, student, research, contractual, legal, and other non-public College information.

Principles for Responsible AI Use

Users of AI technologies shall:

1. Use AI ethically, responsibly, and lawfully.
2. Exercise human judgment when relying upon AI-generated information.
3. Verify AI-generated outputs for accuracy before relying upon them for academic, operational, legal, or institutional purposes.
4. Be transparent regarding AI use whenever disclosure is required by College policy, course requirements, professional standards, or law.

5. Respect privacy, confidentiality, intellectual property rights, and accessibility requirements.
6. Avoid uses that create unlawful discrimination, bias, harassment, misinformation, or other harmful outcomes.

Governance and Oversight

The President shall designate an institutional AI governance structure responsible for:

- reviewing proposed AI technologies;
- evaluating institutional risks;
- recommending approved AI tools;
- monitoring compliance;
- supporting AI literacy and training;
- periodically reviewing this Regulation.

Information Technology shall maintain the College's inventory of approved institutional AI platforms.

The College reserves the right to prohibit or discontinue AI tools that present unacceptable operational, legal, security, ethical, financial, or reputational risks.

Academic Use

Faculty retain authority over the use of AI within their courses consistent with academic freedom and College policy.

Faculty should clearly communicate expectations regarding permissible AI use in coursework.

Students remain responsible for submitting original work consistent with the Academic Integrity Regulation and any course-specific requirements.

AI may assist learning but shall not substitute for demonstration of required knowledge or competencies unless expressly authorized by the instructor.

Administrative and Operational Use

AI technologies may be used to improve administrative efficiency, planning, student services, communications, research, budgeting, institutional effectiveness, and operational processes.

Human oversight shall be maintained for decisions significantly affecting students, employees, or members of the public.

AI shall not serve as the sole basis for disciplinary, employment, admissions, financial aid, or academic decisions.

Research

Researchers utilizing AI shall comply with applicable research ethics, grant requirements, human subjects protections, intellectual property requirements, and data governance standards.

Researchers remain responsible for validating AI-assisted analyses and conclusions.

Data Privacy and Information Security

Users shall not enter, upload, or otherwise expose confidential, proprietary, or personally identifiable information to publicly available or College-unapproved AI tools unless expressly authorized by the College and protected by appropriate contractual safeguards.. The Office of Information Technology in collaboration with the Information Security Standing Committee shall publish and maintain guidance identifying the categories of information that may not be entered into publicly available or College-unapproved AI tools.

All institutional AI systems shall comply with applicable requirements including:

- FERPA
- New Jersey data breach notification laws
- State records retention requirements
- ADA and accessibility requirements
- College cybersecurity standards

Vendor agreements involving AI shall be reviewed through established procurement, information technology, and legal processes.

Intellectual Property

Users shall respect copyright, licensing agreements, and intellectual property rights when using AI technologies.

AI-generated content may not qualify for copyright protection under current United States law absent sufficient human authorship.

Users remain solely responsible for ensuring appropriate attribution, permissions, originality, and compliance with applicable intellectual property laws.

The College assumes no responsibility for ownership disputes arising from AI-generated content.

Approved AI Tools

The Office of Information Technology in collaboration with the Information Security Standing Committee shall maintain and periodically update a list of institutionally approved AI applications and services and communicate to the College community. Only approved AI systems may be used with confidential College information unless an exception has been authorized through established review procedures.

Training

The College shall provide ongoing education regarding:

- responsible AI use;
- AI prompt engineering;
- academic integrity;
- cybersecurity;
- privacy;
- accessibility;
- ethical decision-making; and
- institutional governance.

Units implementing AI technologies are responsible for ensuring appropriate employee training before deployment.

Monitoring and Review

The College shall periodically review AI technologies for:

- effectiveness;
- security;
- legal compliance;
- accessibility;
- bias;
- institutional impact; and
- alignment with strategic goals.

This Regulation shall be reviewed periodically to reflect changes in technology, law, accreditation expectations, and institutional needs.

Violations

Failure to comply with this Regulation may result in disciplinary action under applicable College policies, collective bargaining agreements, student conduct procedures, or contractual provisions.

Violations involving information security, privacy, or misuse of College technology may also be addressed under 2.9000R Computer Resources, Network and Facilities Use Regulation.

V. Responsibility for Implementation

The President has overall responsibility for implementation.

The Office of Information Technology, Academic Affairs, Student Affairs, Planning and Institutional Effectiveness, Human Resources, Finance and Operations, Contract and Legal Administration, and other appropriate administrative units share responsibility for governance, compliance, training, monitoring, and enforcement.

Approved: President, 10/28/2026