YORK College

The City University of New York

OFFICE OF INFORMATION TECHNOLOGY

AI Protocols and Best Practices for York College CUNY

Table of Contents

AI Protocols and Best Practices for York College CUNY

1. Purpose

This document outlines the operational framework for York College's internal AI computing system, designed to manage and analyze student data, as well as data from internal systems. The goal is to ensure safe, ethical, and compliant use of AI technologies, protecting the confidentiality, integrity, and availability of data.

2. Scope

The AI Protocols and Best Practices applies to all staff, faculty, and authorized users interacting with the AI system. It covers:

- Data management and analytics
- Access control
- Change management
- Security and privacy measures

In the event any provision of this document conflicts with University Policy or applicable law, the University Policy and/or applicable law govern.

3. AI Oversight Committee

The AI Oversight Committee is responsible for overseeing the development, deployment, and monitoring of AI systems and their outputs. Its duties include:

- Establishing ethical standards for AI use
- Ensuring compliance with legal, ethical, and institutional policies
- Overseeing data security and privacy
- Monitoring the performance and impact of AI models

Access to AI Computing System

1. Eligibility

Access to the AI system is limited to authorized personnel whose roles require interaction with the system for academic, research, or administrative purposes. This includes faculty, staff, and approved external consultants.[1]

2. Requesting Access

- Requests for access must be submitted through a formal process, including justification for access, the nature of the data to be accessed, and required access levels.
- The AI Governance Committee, in collaboration with the IT department, will review and approve access requests based on job roles and responsibilities, as outlined in the

[1] Outside entities given access to the College's AI System must agree to maintain confidentiality of student records, at a minimum, in compliance with the requirements of the Family Educational Rights and Privacy Act (FERPA).

institution’s Data Classification Standards (Non-public data disclos…)(Information-Security-Re…).

3. Levels of Access

- Access is role-based and divided into categories such as read-only, data analysis, and full administrative control. Each category comes with distinct privileges.
- Administrative access will only be granted when necessary, following the principle of least privilege (Local-Administrative-Pr…).

4. Data Use and Compliance

Users are responsible for ensuring that the data they access is used in compliance with York College’s Acceptable Use Policy and CUNY’s policies (CUNY-Acceptable-Use-of-…) (Computer-Use-1). Misuse of AI data may result in removal of access, as well as disciplinary and/or legal actions.

Change Management

1. Change Control Procedure

- All modifications to the AI computing system, including updates to algorithms, configurations, and data sets, must follow the established Change Management Procedure.
- A formal change request must be submitted to the AI Oversight Committee, detailing the scope of changes, the rationale, and potential impacts on security, privacy, and compliance (CUNY-Acceptable-Use-of-…)(Cybersecurity-Risk-Acce…).

2. Risk Assessment

Each change will undergo a risk assessment, following the risk acceptance procedures, to evaluate potential impacts on data security, system integrity, and compliance. The AI Oversight Committee will approve or deny changes based on this assessment(Cybersecurity-Risk-Acce…) (Information-Security-Re…).

3. Audit Trails

All changes to the system will be logged and audited, with detailed records of the person initiating the change, the nature of the change, and its impact (Non-public data disclos…) (Information-Security-Re…).

Data Safeguards and Security

1. Data Classification

All data processed by the AI system must be classified according to CUNY’s Data Classification Standard, ensuring appropriate safeguards are in place based on the data's sensitivity (CUNY-Acceptable-Use-of-…)(Non-public data disclos…).

2. Encryption

Data at rest and in transit must be encrypted using industry-standard encryption protocols to protect confidentiality and integrity (CUNY-Acceptable-Use-of-…)(Non-public data disclos…).

3. Access Control

Multi-factor authentication (MFA) will be mandatory for accessing the AI system. Only authorized users will have access to non-public data, and access will be reviewed regularly (Non-public data disclos…)(Information-Security-Re…).

4. Incident Response

Any security incidents involving the AI system must follow the established Incident Response Procedure, which includes immediate notification to IT security teams and the AI Oversight Committee (IT-Security-Procedures-…).

Monitoring and Auditing

The AI system will be continuously monitored for unauthorized access or unusual activity. Detailed audit logs must be maintained to trace access, usage, and modifications. These logs must be securely stored and reviewed regularly by the IT department and the AI Oversight Committee (Non-public data disclos…)(Information-Security-Re…).

Training and Awareness

All personnel with access to the AI system must undergo mandatory training in AI ethics, data privacy, and cybersecurity, ensuring they are aware of their responsibilities and the risks associated with handling sensitive data (CUNY-Acceptable-Use-of-…)(IT-Security-Procedures-…).

These AI Protocols and Best Practices provide the structure for managing AI technologies at York College CUNY, ensuring ethical use and compliance with institutional and legal standards. It promotes transparency, security, and accountability in the use of AI systems.

YORK
College

Greg Vega
Interim AVP/CIO
York College Information Technology
718-262-5231
gvega@york.cuny.edu