Status Draft PolicyStat ID 19722859

| | |
|---|---|
| Last Approved | N/A |
| Effective | N/A |
| Next Review | N/A |
| Area | Information Technology/ Management (Procedures) |
| Chief Or Responsible Office | Chief Information Officer |

# Artificial Intelligence (AI) Usage

Authority for Procedure granted by UWG Policy #5004 University Artificial Intelligence (AI).

# A. Purpose and Scope

This procedure establishes a framework for the responsible use of Artificial Intelligence (AI) Tools at the University of West Georgia (UWG) across academic, administrative, research, and operational functions. It is intended to guide appropriate adoption, promote transparency, protect Data, and ensure compliance with legal and institutional standards. Given the rapid pace of AI development, this procedure will evolve in response to emerging AI Technologies and feedback from the University Community.

# B. AI Tool Inventory

## 1. Inventory Requirements

All AI tools used within UWG contexts, including installed or offline models that also present security or compliance risks, shall be documented in an institutional inventory. This inventory must include, but is not limited to, the following Data elements:

- **Tool Name**
- **Vendor**
- **AI Tool Type** (e.g., chatbot, Generative AI, embedded vendor AI agent)
- **AI Model Type** (e.g., large language model (LLM), image generator, recommendation engine)
- **Description of Data Interaction** (e.g., interaction with institutional or student Data)
- **Data Storage** (physical location of Data servers or centers)
- **AI Security** (security practices and risk considerations)
- **Purpose/Organizational Benefit**

## a. Inventory Support Materials and Guidance

To support the University Community's use of approved AI tools responsibly and in compliance with policy, Information Technology Services (ITS), the Office of the Vice President for Academic Affairs (VPAA) / Academic Affairs, the Office of Legal Affairs (OLA), the Institutional Record of Processing Activity (RoPA) Owner, and/or applicable Data Stewards may create, maintain, and update handbooks, user manuals, FAQs, and other guidance materials. These resources must be reviewed annually and updated to reflect changes in AI Tools, regulations, or University policy and made accessible through official University channels.

In the event of conflict between these support materials and **UWG Policy #5004 University Artificial Intelligence (AI) and its associated procedures**, the Policy and procedures shall prevail.

# 2. AI Tool Inventory Review Process

To ensure responsible use and alignment with evolving AI Technologies and regulations, UWG will maintain a structured, recurring review process for the institutional AI Tool Inventory.

i. **Inventory Review Frequency and Scope**
The AI Tool inventory will be reviewed at least annually by Information Technology Services (ITS). Additional reviews will be conducted immediately in response to:

- Significant advancements or changes in AI tools or capabilities.
- Updates to relevant federal, state, or international regulations (e.g., FERPA, GDPR, CCPA).
- Changes in institutional strategies or academic/operational priorities.
- New guidance or mandates from the Board of Regents (BOR) or the University System of Georgia (USG).

Each review will evaluate the following:

- **Accuracy and completeness** of inventory entries (e.g., tool name, vendor, AI type, Data interaction, etc.)
- **Alignment with institutional goals**, values, and standards.
- **Legal and privacy compliance** with applicable laws and university policies.
- **Performance and reliability** of AI tools, including any reported or documented issues.
- **Vendor assurances** of ethical AI use and Data protection standards.

ii. **Inventory Review Process**
Oversight of the review process and implementation of AI policy and procedures resides with the Chief Information Officer (CIO) in collaboration with the Chief Academic Officer and Chief Legal Officer.

Other responsible University Units may include, but are not limited to, Internal Audit, Office of

Human Resources, Academic Affairs Division, Institute for Faculty Excellence, and Faculty Senate.

Each division and department is responsible for submitting updates or changes to their AI tool usage for review.

iii. **Documentation and Reporting**
A formal review report will be compiled after each review cycle. This report will:

- Summarize findings, inventory updates, and any recommendations.
- Be submitted to the Office of the President and the Faculty Senate.
- Be made publicly available to the University Community via the ITS website.

AI Tools identified as non-compliant or obsolete will be flagged for remediation or removal from the inventory.

# C. Ethical Use of AI Tools

UWG is committed to ensuring AI Tools used in operational, academic, and research contexts reflect the highest standards of integrity and responsibility.

# 1. Core Principles for Ethical AI Use

All AI Tools must align with the following guiding principles:

i. **Fairness and Bias Mitigation:** Tools must be evaluated for potential biases in their design, training Data, and outputs. The university prioritizes AI Tools that demonstrate efforts to reduce bias.

ii. **Accountability:** Clear lines of accountability must be established for the use of AI Tools. The University Community is accountable for the ethical use and oversight of AI Tools, and vendors must offer transparent documentation on tool functionality, development, and maintenance.

iii. **Accuracy:** AI Tools must be assessed for factual accuracy and reliability. Tools that consistently generate false or misleading content (commonly referred to as “Hallucinations”) will be subject to heightened scrutiny and/or may be restricted from use.

iv. **Transparency:** The functionality, limitations, and decision-making processes of AI Tools must be documented and communicated to Users. This includes disclosure of AI-generated content in academic work and research.

v. **Human Oversight:** AI must assist, not replace, human judgment with all outputs reviewed by a human decision-maker. Users remain ultimately responsible for decisions and outputs generated with the assistance of AI Tools.

vi. **Accessibility:** AI Tools must meet accessibility standards to ensure usability by all members of the University Community. Vendors must provide evidence and/or assurances that their Tool meets accessibility standards.

vii. **Security:** AI Tools must be evaluated for vulnerabilities, including susceptibility to Prompt Injection attacks or manipulation. Vendors must provide evidence of security measures or

safeguards to mitigate such risks.

## 2. Implementation and Oversight Measures

To uphold the University's standards for ethical, secure, and responsible AI use, UWG will implement the following measures:

i. **AI Procurement, Contract Review, and Cybersecurity Oversight**
All AI Tools procured, licensed, or otherwise acquired by the University shall comply with University System of Georgia requirements and USG Business Procedures Manual **BPM 3.4.4, Supplier Contracts**.

During procurement or renewal, AI vendors must provide documentation demonstrating compliance with ethical, legal, accessibility, and security standards.

Any AI Tool that collects, processes, stores, or accesses Sensitive, Confidential, or protected Data requires documented review and approval by:

- Information Technology Services (ITS), including a cybersecurity review;
- Procurement Services; and
- The Office of Legal Affairs (OLA).

AI Tools subject to this enhanced review will undergo **annual cybersecurity and risk assessments** conducted by ITS to ensure ongoing compliance with security, privacy, and data protection standards. Tools failing to meet these requirements may be restricted, remediated, or removed from approved use.

ii. **Governance and Audit**
The UWG Data Governance Committee will conduct Periodically audits and reviews of AI Tools to assess continued alignment with ethical standards. The committee will also evaluate new tools and address ethical concerns.

iii. **Education Support**
ITS will offer training and resources to leadership, faculty, staff, and students on responsible AI use.

iv. **AI Tool Registry**
ITS will maintain a publicly accessible registry of approved AI Tools, including usage guidelines, assessments, and links to related documentation.

# D. Acceptable Use and Disclosure

## 1. User Responsibilities

All members of the University Community who use Artificial Intelligence (AI) Tools, including immersive tools (e.g., Apple Vision Pro, Meta Quest Goggles) and other experiential classroom learning tools, are responsible for their ethical and lawful use. Users must:

i. **Confirm Accuracy and Legality:** Do not rely solely on AI-generated content. Always verify

information using credible sources, as AI outputs can be inaccurate, biased, misleading, or fabricated ("Hallucinations").
***Note:*** *AI-generated content may contain copyrighted material. Users are responsible for any legal consequences of publishing such content.*

ii. **Evaluate for Bias or Discrimination:** Review AI outputs for bias or disparate impacts based on protected classifications (i.e., race, color, sex, pregnancy, ethnicity or national origin, disability, religion, age, genetic information, veteran status, or any other characteristic protected by institutional policy or state, local, or federal law). Disregard any output that is indicative of a potential bias.

iii. **Disclose AI Use Transparently:** Clearly disclose when AI Tools are used to generate academic or professional work. Transparency ensures academic integrity and fosters trust.

iv. **Avoid Misuse or Legal Violations:** Do not use AI to plagiarize, mislead, or violate intellectual property rights, laws, or university policies. Confirm that any quoted or paraphrased content is accurate, properly cited, and does not plagiarize or violate intellectual property rights.

v. **Prohibit Malicious Use:** AI must not be used to generate harmful content, such as malware or code intended to bypass security controls.

# 2. Data Protection Requirements

Users **must not** input Confidential, Sensitive, or PII information into AI Tools unless authorized through an appropriate contract and security review.

**Prohibited input includes:**

- **Confidential Information** (e.g., Sensitive research Data or legally protected information)
- **Personal Information** about students, faculty, staff, or other stakeholders
- **Copyrighted or Licensed Content** without proper usage rights
- **Intellectual Property or Proprietary Information** (e.g., proprietary research or patentable ideas)

When possible, opt out of allowing AI Tools to retain or use inputs for training purposes.

# 3. Academic Integrity and Research Use

i. **Students**
    - Must adhere to guidelines for acceptable use, avoiding prohibited AI Tools.
    - Must comply with UWG's AI and Academic Integrity policies, procedures, and guidelines.
    - Must only use UWG-approved AI Tools on UWG devices. AI Tools used on personal devices must be authorized by the instructor for the respective course and must follow course-specific guidelines.
    - Use of prohibited AI Tools or failure to properly disclose AI assistance may constitute academic misconduct.

ii. **Instructors**

- Should clearly define expectations by defining permitted and prohibited AI use in syllabi and coursework.
- Must obtain approval from ITS at least 30 days before implementing any AI Tools to ensure adequate vetting.
- Are encouraged to foster responsible engagement with AI in learning contexts.

iii. **Researchers**

- Must disclose AI use in research design, methodology, analysis, and writing.
- Attribution is required in publications, grant submissions, and collaborative projects.

***[Refer to the Guidelines and Related materials, Faculty Handbook, Student Handbook, and USG policy for detailed academic guidelines.]***

# 4. Allowable Tools

The institution will define and regularly update a list of University-approved AI Tools on the ITS website. Exceptions for new or specialized Tools may be submitted for review to the AI Data Governance Committee or via a designated intake process.

Students must refer to AI guidelines within each course syllabus for the courses they take.

# 5. Monitoring and Validation

Users are responsible for validating the outputs of AI Tools and report any discrepancies or issues to ITS.

ITS is responsible for monitoring AI Tools to ensure they function as intended and resolve any discrepancies or issues promptly.

# 6. AI Tool Documentation / Disclosure Standards

## a. Standardized Templates and Examples

The University shall maintain standardized templates and/or examples for required AI disclosures and related documentation, including, as applicable:

- Academic use disclosures
- Research attribution statements
- Operational or administrative AI use documentation

These templates and/or examples shall be **developed and maintained by the appropriate unit authority** (e.g., Academic Affairs, ITS, Research and Sponsored Operations (ORSP)), and shall be made available through official UWG websites or incorporated into institutional handbooks and/or guidance materials.

Templates and examples may be revised as necessary to ensure compliance with applicable law, USG and BOR requirements, and institutional standards, and are incorporated by reference into this

Procedure. ***[Refer to the Guidelines and Related materials, Faculty Handbook, Student Handbook, and USG policy for detailed academic guidelines.]***

## b. AI Tool Usage Disclosure Requirement

All AI Tool usage across administrative, operational, non-academic, academic, and research contexts must be documented at a level sufficient to demonstrate compliance with this Procedure, University objectives, and all applicable legal or regulatory requirements.

**Minimum documentation shall include:**

1. **AI Tool name and vendor**
2. **Purpose and business function supported**
3. **Type and classification of data processed**
4. **Confirmation of required approvals and reviews**
5. **Description of human oversight applied to AI outputs**

## c. Sample AI Tool Output Disclosure Statements

### i. Administrative, Operational, and Non-Academic AI Outputs:

> "The University utilizes **[AI Tool Name]**, provided by **[Vendor Name]**, to support **[specific purpose or business function]**. The system processes **[type of data]**, classified as **[data classification level]** under University data governance standards. All required approvals and reviews, including legal, privacy, security, and procurement reviews, have been completed prior to use. AI-generated outputs are subject to human oversight, including review and validation by **[responsible role or unit]**, and final decisions remain under human authority."

### ii. Academic or Research AI Outputs:

> "This research project utilized **[AI Tool Name]**, provided by **[Vendor Name]**, to support **[specific research or academic activity]**. Portions of the content, data analysis, or writing were generated or influenced by the AI tool. All AI-generated outputs were reviewed and validated by **[researcher's name or team]** to ensure accuracy, compliance with academic standards, and integrity of the final work product."

## d. Records Retention and Access

All AI documentation, including disclosure statements, templates, and validation records, shall be retained in accordance with the USG Records Retention Schedules. Such documentation must be made available upon request for audit, compliance review, or risk assessment purposes.

# E. Training and Awareness

## 1. AI Training Requirements

The university shall provide training to employees and raise student awareness about responsible and ethical use of Artificial Intelligence (AI). This training will ensure that all members of the University Community understand the risks, responsibilities, and regulatory requirements associated with AI Tools.

i. **Training Objectives**

- Promoting ethical AI use, including principles of fairness, accountability, transparency, and human oversight.
- Raising awareness of potential risks such as bias, Hallucinations, Data misuse, and Prompt Injection vulnerabilities.
- Clarifying expectations for responsible AI use across teaching, learning, research, operations, and communication.
- Ensuring understanding and adherence to relevant laws and university policies.

ii. **Training Delivery and Compliance**

- **Audience:** All employees and student-workers/employees
- **Frequency:** Mandatory upon onboarding and annually thereafter
- **Format:** Online modules, in-person workshops, and department-specific sessions
- **Tracking:** The Office of ITS/Cybersecurity, in collaboration with OHR, will monitor completion with non-compliance addressed through divisional and departmental leadership.

## 2. Policy Awareness Strategy and Communication

To ensure University-wide compliance with the AI Policy, the following awareness strategies shall be implemented, documented, and coordinated by designated responsible personnel. Responsibility for policy awareness and communication is shared among all University personnel, and students responsible for engaging with or the use of AI Tools in accordance with this Policy.

The following **Awareness Strategies** shall be implemented and documented to ensure University-wide compliance:

- **Policy Publication:** Publish the AI Policy in the University PolicyStat Library, with supporting materials and guidance made available and accessible to the University Community through institutional webpages and handbooks.
- **Communications:** Disseminate campus-wide announcements regarding the AI Policy through newsletters, faculty/staff meetings, and other official communication channels. Ensure updates are included in divisional communications, student and employee orientation, and faculty development sessions.
- **Integration into Academic and Operational Activities:** Incorporate key AI Policy points into course syllabi, program guidelines, and operational workflows where AI tools are used.

- **Training and Documentation:** Require all personnel to complete annual mandatory AI training and maintain documentation of completion.
- **Departmental Liaison Engagement:** Designate AI Liaisons to serve as local points of contact and policy ambassadors for compliance matters within their units. Liaisons shall facilitate departmental communications and assist personnel with AI Policy guidance.

These strategies, implemented through coordinated efforts, shall ensure the University Community is informed, trained, and equipped to engage with AI tools responsibly and in compliance with University policies. Records of communications, training, and outreach activities shall be maintained in accordance with University records retention schedules and made available for audit or review. ***[For detailed information on Training and Awareness roles and responsibilities, see Section G.2, Governance and Oversight.]***

# F. Legal and Regulatory Compliance

## 1. Compliance with Laws and Standards

All AI Tools must comply with:

- Applicable federal, state, and international laws.
- University policies and procedures.
- Industry standards for responsible and ethical AI use.

Any AI Tool that collects, shares, or processes protected or Sensitive Data must undergo a thorough review to ensure compliance with legal and regulatory requirements before it is approved for use.

## 2. Data Privacy and Protection

To protect institutional and student Data, the following requirements apply:

- AI Tools must **only collect, process, and store Data** necessary for their intended purpose.
- Special attention should be paid to prevent the unintentional sharing of Personally Identifiable Information (PII), including student work or other Sensitive or protected Data.
- Data shall be handled in accordance with the **USG and UWG Data governance policies** and applicable **privacy laws**.
- Vendors must provide clear, written documentation outlining how Data are **collected, used, stored, and protected**.

***Reference:*** *University System of Georgia Business Procedures Manual (BPM) Section 12.6 Data Privacy.*

## 3. Vendor and Tool Evaluation

Before adoption, AI Tools must undergo a compliance and risk assessment review. This includes:

- A **Data Protection Impact Assessment (DPIA)** for Tools processing Sensitive or large-scale personal Data.
- A **Security and Privacy Review** conducted by the Information Technology Services (ITS).

- A **Legal Review** by the Office of Legal Affairs to ensure contractual and regulatory compliance.

**Vendors must provide:**

- **Documentation demonstrating compliance** with relevant laws and standards.
- A **Data Processing Agreement (DPA)** outlining responsibilities and safeguards.
- Written assurance that Data **will not be used for unauthorized purposes**, including training unrelated AI models.

## 4. Roles and Responsibilities

Oversight and compliance responsibilities are shared among the following roles and offices:

- **Office of Legal Affairs (OLA):** Monitors regulatory developments and revises institutional policies accordingly.
- **Information Technology Services (ITS):** Conduct vendor assessments and risk evaluations for AI Tools prior to adoption.
- **Institutional Record of Processing Activity (RoPA) Owner:** Reviews or delegates privacy compliance reviews for Data processing AI Tools.
- **AI Liaisons (Unit-Level):** Ensures departmental (local) compliance and reports concerns to administration.

# G. Governance and Oversight

## 1. Points of Contact

To ensure effective coordination and support, UWG designates both institutional and departmental points of contact for AI governance:

i. **Institutional Lead**: **Chief Information Officer (CIO)**
Serves as the primary lead for institutional oversight of AI policy and implementation.

ii. **Unit Contacts: AI Liaisons**
Appointed within each division, college, school, or operational unit to serve as the primary contact for departmental AI use. Liaisons provide feedback based on departmental experiences and needs, ensure compliance, and assist with implementation at the local level.

## 2. Roles and Responsibilities

The following offices and individuals share responsibility for reviewing, implementing, and supporting UWG's AI policy and procedures:

i. **Information Technology Services (ITS):** Serves as the **Institutional Oversight Authority** for enterprise AI Tools and is responsible for evaluating, approving, and monitoring AI Technologies; Leads AI policy implementation; Coordinates stakeholder input; Communicates institutional AI guidance; Oversees mandatory training; Maintains records and approves AI Tool use in alignment with institutional standards and priorities.

ii. **Data Privacy Personnel & Data Governance Committees:** Assess compliance with Data

protection standards and ensure responsible handling of Confidential or Sensitive information in AI Tools.

iii. **Office of Community Standards:** Promotes responsible student use of AI in alignment with the Student Code of Conduct (Wolf Code); Collaborates with Academic Affairs and ITS on student-facing AI awareness initiatives; Supports educational outreach on University Community values, conflict resolution, and accountability.

iv. **Office of Human Resources (OHR):** Provides input on AI use in personnel-related matters; Integrates AI policy requirements into onboarding, orientation, and professional development; Coordinates with ITS and Academic Affairs to deliver, track, and document mandatory AI training.

v. **Office of Legal Affairs (OLA):** Ensures regulatory compliance with applicable laws and USG policies; Reviews AI-related contracts and vendor terms; Advises on legal and ethical risks associated with AI technologies.

vi. **Office of the Vice President for Academic Affairs (VPAA) / Academic Affairs:** Provides discipline-specific guidance on the use of AI in teaching, learning, and scholarship; Integrates AI policy requirements into academic policies, guidelines, instructional materials, and faculty development; Assesses emerging academic AI practices and recommends policy or procedural updates; Delivers faculty-focused AI training.

vii. **Supervisors, Faculty, and Departmental AI Liaisons:** Serves as local points of contact and policy ambassadors; Communicates AI policy expectations; Integrates AI requirements into departmental and instructional practices; Guides faculty/staff/student responsible on AI use; Suggests changes to AI policies or procedures when needed; Reports any AI use that may violate policy or create compliance, ethical, or legal concerns.

## 3. Complaint Resolution

i. **Academic Context:** Complaints related to AI misuse in academic settings may be reported to the Office of Community Standards. (See UWG Student Conduct Code (aka Wolf Code), Section 2.00. Academic Dishonesty)

ii. **Operational/Non-Academic Contexts:** Complaints involving AI use in administrative or operational contexts will be addressed by the Office of Cybersecurity, in collaboration with OHR and OLA.

# H. Policy and Procedure Review

In recognition of the rapid evolution of AI Technologies and the potential risks they present, UWG is committed to maintaining a current and responsive AI policy, along with supporting procedures and guidelines.

To ensure continued relevance, effectiveness, and legal compliance:

- The University Community is encouraged to review UWG's AI Policy, related procedures, and published guidance regularly and frequently.
- The University Community is expected to follow UWG's AI Policy, related procedures, and official guidance when using AI in any work or education-related activities.

All proposed revisions to this procedure shall follow the official UWG Policy and Procedure Review Process as outlined in UWG PL 1002: Policy and Procedure Development.

This procedure will be reviewed annually, in conjunction with the AI Policy or more frequently as needed in response to changes in laws, technologies, institutional priorities, or the risk environment.

All revisions will be evaluated through the appropriate administrative channels to ensure alignment with institutional goals, applicable laws, and higher education best practices.

# I. Compliance

## 1. Reporting Misuse or Violations

Any suspected misuse of AI Tools or violations of this procedure by **employees** should be reported to:

> **Information Technology Services (ITS)**
> Phone: (678) 839-6587
> Email: servicedesk@westga.edu

Any suspected misuse of AI Tools or violations of this procedure by **students** should be reported to:

> **Office of Community Standards**
> Phone: (678) 839-2466
> Email: ocs@westga.edu

## 2. Disciplinary Actions

Non-compliance with this procedure may result in disciplinary action, which may include, but is not limited to:

- Formal warnings or written reprimands
- Suspension or revocation of access to university-provided devices, systems, or services
- Termination of employment or contractual agreements

All disciplinary measures will be administered in accordance with UWG policies, relevant employee handbooks, and applicable federal and state laws.

# Definitions

**Artificial Intelligence (AI)** - technologies that enable computers to perform a variety of advanced functions, including the ability to process visual cues, understand and translate spoken and written language, analyze data, and make recommendations from heuristic analyses.

**AI Tools / Technologies** - software and/or services or hardware systems that utilize AI technologies.

**Confidential Information** - information maintained by the institution that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

**Data** - information collected, processed, or stored by AI systems.

**Generative AI** - a form of AI capable of generating text, images, videos, or other data using generative models, often in response to prompts.

**Hallucinations** - conditions when a large language model (LLM) process identifies patterns or objects that are nonexistent, creating nonsensical or inaccurate outputs.

**Periodically** - for the purposes of this procedure, periodically is defined as: at a minimum, annually or immediately upon the occurrence of any of the following:

- Significant advancements or changes in AI technologies
- Updates to federal, state, or international laws and regulations
- Revisions to institutional strategy or academic priorities
- New guidance or mandates issued by the Board of Regents (BOR)

**Personally Identifiable Information (PII)** - any information that can be used to identify an individual, either directly or indirectly. This includes names, identification numbers, addresses, and other data linked to a person, regardless of their citizenship or affiliation with the institution.

- **Sensitive Personally Identifiable Information (Sensitive PII)** - a subset of PII that, if disclosed without authorization, could cause significant harm, embarrassment, disruption, or unfairness to the individual, such as Social Security numbers or immigration identification numbers. Sensitive PII requires stricter protection and handling due to the increased risk if compromised.

**Prompt injection** - a specialized type of cyber-attack against large language models (LLM), whereby bad actors disguise malicious inputs as legitimate, resulting in the return of erroneous results or leaking sensitive information.

**Sensitive Information** - any data maintained by the institution that requires special precautions to protect it from unauthorized access, use, disclosure, modification, loss, or deletion. This includes both public and Confidential Information that demands a higher-than-normal level of assurance regarding its accuracy, completeness, and security due to its potential impact if compromised.

**University Units** - any institutional department or office that reports through the chain-of-authority to the University President, including divisions, colleges, schools, departments, and offices. For the sake of this procedure, committees and task forces may be considered university units if they are operating in accordance with their charters, approved by a division vice president.

**University Community** - (1) All persons enrolled at or employed by the University, including University students, faculty, staff, administrators, and employees, and (2) recognized University-affiliated entities including University departments, foundations, and registered University student organizations.

**User** - anyone using the University of West Georgia's Information Technology Facilities or accounts.

# Guidelines and Related materials

UWG Community members must also follow applicable USG and University policies and procedures, including:

- **University System of Georgia**
    - USG Policy Manual, Section 6.28 Artificial Intelligence in Academic Contexts
    - USG Information Technology Handbook
    - Artificial Intelligence: A USG IT Handbook Guide
- **University of West Georgia**
    - **Handbooks**
    - UWG Faculty Handbook
        - 200 Policies and Procedures Related to Teaching Responsibilities
        - 201 Classroom Procedures
        - 206 Academic Honesty/Dishonesty
    - UWG Student Handbook and Wolf Code
    - UWG Employee Handbook
    - For Faculty: Institute for Faculty Excellence webpage for academic AI-approved guidance, templates, and examples.
- UWG PL 5003 Privacy
    - Family Educational Rights and Privacy Act (FERPA)
    - EU General Data Protection Regulation Compliance (GDPR)
- UWG PL 1012 Intellectual Property (IP) and associated procedures
- UWG PL 4002 Non-Discrimination / Anti-Harassment
    - Non-Discrimination and Anti Harassment Complaint Procedure
- California Consumer Privacy Act (CCPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA) (where applicable)
- National Institute of Standards and Technology (NIST) AI Risk Management Framework

For questions or policy guidance, visit: UWG AI Policy Page

## Approval Signatures

| Step Description | Approver | Date |
|---|---|---|