AI Usage Guidelines for Staff

Important: How This Document Relates to the AI Security and Risk Policy

The Morehouse College AI Security and Risk Policy defines the formal rules, controls, and governance framework for all AI use at the College. These Guidelines translate those requirements into clear, day-to-day behavioral guidance for staff. Both documents are in effect. In the event of a conflict, the AI Security and Risk Policy governs. A copy of the Policy is available on the ITS intranet page or by visiting servicedesk.morehouse.edu.

These guidelines reflect current expectations and will continue to evolve as institutional AI policies, approved tools, and governance structures develop.

1. Introduction

Artificial intelligence tools are increasingly embedded in how administrative and operational work gets done across higher education. At Morehouse College, AI is recognized as a strategic asset that, used responsibly, can enhance staff productivity, support the College's mission, and improve service delivery to students, faculty, and the broader community.

These guidelines apply to all non-faculty staff employed by Morehouse College, including full-time and part-time employees, as well as contractors or temporary staff who access College systems or data. They govern the use of any AI tool in the performance of College work, whether accessed through a College-provisioned account or through a personal account.

These guidelines apply to administrative and operational decisions. Academic uses of AI in teaching, learning, and research, including grading and student evaluation, are governed by the Morehouse College Academic AI Guidelines.

2. Definitions

The following terms are used throughout this document.

Artificial Intelligence (AI)	Software systems that perform tasks typically associated with human cognition, including natural language generation, summarization, translation, image creation, data analysis, and decision support.
Enterprise AI Tool	An AI tool provisioned, licensed, or approved by Morehouse College ITS for institutional use, accessed through a College account with data governance controls in place.
Consumer AI Tool	An AI tool accessed via a personal account or a free web interface, not provisioned by the College. Examples include ChatGPT accessed at chat.openai.com with a personal account, or Google Gemini accessed via a personal Gmail account.

Sensitive Data	Any information is subject to legal, regulatory, or institutional protection. Corresponds to Tier 1 Restricted and Tier 2 Confidential classifications. See Section 6 for the full classification table.
AI-Generated Content	Any text, image, data, code, or other output produced in whole or in substantial part by an AI tool.
Human Review	The act of a qualified Morehouse employee reading, evaluating, and taking responsibility for AI-generated content before it is submitted, sent, acted upon, or filed.

3. Guiding Principles

These principles align with the College's institutional standards for Responsible AI use as defined by the AI Security and Risk Policy and are translated here into day-to-day expectations for staff work.

All staff use of AI at Morehouse College should reflect the following principles. These are not aspirational statements; they carry practical meaning for how you use these tools every day.

Privacy

AI tools, especially consumer-grade tools, may store, log, or use the content you enter to improve their models. You are responsible for ensuring that no personally identifiable information, student records, HR data, financial data, or other sensitive information is entered into any AI system unless that system has been explicitly approved for that data type. When in doubt, do not input it.

Security

Using an unapproved AI tool may introduce data security risks. Only tools on the approved list may be used for College work. Unapproved tools have not been reviewed for compliance with FERPA, HIPAA, institutional data agreements, or Morehouse's vendor management requirements. Only tools on the approved list may be used for College work.

Transparency

If you use AI to produce content that will be submitted as your work, shared with colleagues or supervisors, or sent externally to students, parents, donors, or vendors, you should be prepared to disclose that AI assistance was used. You do not need to flag every use of AI for spell-checking or grammar. Still, substantive AI-generated drafts, analyses, or recommendations should be identified as such when they inform a consequential decision or communication. Your supervisor may have additional expectations for your department.

Accountability

You are responsible for every output you submit or act on, regardless of whether AI produced it. AI tools make errors. They can generate confident-sounding statements that are factually wrong, fabricate citations, misrepresent data, and reflect historical biases in their training data. Reviewing and verifying AI output before using it is not optional; it is part of the work.

Fairness

AI systems can reflect and amplify biases related to race, gender, socioeconomic background, and other protected characteristics. This is particularly relevant at Morehouse, where the mission

centers on the education and advancement of Black men and the broader community we serve. Do not use AI to rank, score, filter, or evaluate people in ways that could introduce or reinforce bias. If you are using AI in a context that involves student outcomes, hiring, or financial aid, consult your supervisor and ITS before proceeding. These expectations apply to administrative and operational decision-making. Academic uses of AI in grading, assessment, and instruction are governed separately by the Academic AI Guidelines.

Reliability

AI tools are useful aids, not authoritative sources. Do not cite AI-generated content as a source of facts without independently verifying the underlying information. Do not present AI output as research, legal guidance, financial advice, or medical information.

4. Approved Tools

Only tools that have been reviewed and approved by ITS may be used for College business. The current approved tool list is maintained on the ITS intranet page and is updated as new tools are evaluated. Staff should check the list before using any AI product, including products embedded within software the College already licenses (such as AI features in Microsoft 365 or Google Workspace). Tool approval, data classification alignment, and compliance review are governed by the AI Security and Risk Policy.

4.1 Currently Approved Tools

The table below reflects the tools approved as of the effective date of these guidelines. This list will be updated as additional tools are reviewed and approved or deprecated.

Tool	Access Method	Approved Use Cases	Data Restrictions
Microsoft Copilot (M365)	College M365 account only	Drafting, summarizing, emailing, scheduling, and data analysis within M365 apps	No Tier 1 Restricted or Tier 2 Confidential data. See Section 6.
Google Gemini (Workspace)	College Google Workspace account only	Drafting, summarizing, and research support within Google Workspace apps	No Tier 1 Restricted or Tier 2 Confidential data. See Section 6.

Note: AI features embedded in existing licensed software (for example, Copilot features in Word, Outlook, or Teams) are covered under the enterprise tool approval for that platform, provided you are accessing them through your College account. Using the same tool through a personal account is not covered.

4.2 Requesting Approval for a New Tool

If you identify an AI tool you believe would benefit your work, and it is not on the approved list, you may submit a tool evaluation request to ITS. The process is as follows:

1. Submit a request via the ITS Service Portal (TDX) using the AI Tool Evaluation Request form.
2. ITS will conduct a review covering data privacy, security, vendor agreements, and compliance requirements.
3. The review process targets a 15-business-day turnaround for standard requests.
4. ITS will notify you of the outcome and, if approved, provide access instructions.

Do not begin using a tool while an evaluation request is pending.

5. Approved Uses

The following categories of use are approved for staff using tools on the current approved list, subject to the data restrictions in Section 6. These are illustrative examples, not an exhaustive list. If your intended use is not clearly covered by one of these categories, contact ITS or your supervisor before proceeding.

5.1 Communication Drafting

Staff may use AI tools to draft, edit, or improve written communications, including emails, letters, announcements, and internal memos. The staff member must review the final content before sending. AI-generated communications sent to students, parents, donors, or external partners must reflect accurate information and must not misrepresent College policies or commitments.

5.2 Document Summarization

AI tools may be used to summarize publicly available documents, research reports, non-sensitive meeting notes, or other non-protected materials. Do not upload full documents that contain sensitive data, even if you only want a summary of a portion of the document. Remove or redact sensitive information before using AI summarization tools.

5.3 Administrative Workflow Support

AI tools may assist with tasks such as creating meeting agendas, organizing project plans, generating draft procedures or checklists, and formatting data that does not contain sensitive information. Any output that becomes part of an official College record must be reviewed and approved by the staff member responsible for that record.

5.4 Research and Brainstorming

AI tools may be used to generate ideas, explore problem-solving approaches, draft talking points, or research general topics. AI-generated research must be independently verified before being relied upon. AI tools are not a substitute for primary sources, and any factual claims derived from AI tools must be confirmed with authoritative sources.

5.5 Accessibility Support

AI tools may be used to support accessibility needs, including generating captions, creating alternative text for images, or reformatting content for readability. This use is encouraged where it supports inclusive service delivery.

6. Data Classification and AI Use Restrictions

This section summarizes AI-specific expectations derived from the Morehouse College Data Security and Classification Policy and the AI Security and Risk Policy.

Morehouse College classifies institutional data into four tiers as defined in the Data Security and Classification Policy (Version 2.0). Your obligation when using AI tools depends on the classification tier of the data involved. When in doubt about how a piece of information is classified, treat it as Tier 1 Restricted and contact ITS before proceeding.

The full classification framework, including detailed examples and handling controls, is defined in the Data Security and Classification Policy. This section summarizes the AI-specific use rules for each tier.

Tier	Description and Examples	Regulations / Risk	AI Use Rule
Tier 1: Restricted	Highest sensitivity. Information subject to legal or regulatory protection. Includes: student educational records (FERPA), Social Security numbers, financial account data, Protected Health Information (HIPAA), NPI (GLBA), biometric identifiers, attorney-client communications, and security vulnerability information.	FERPA, HIPAA, GLBA, PCI-DSS, state law	NEVER enter into any AI tool under any circumstances.
Tier 2: Confidential	Sensitive institutional information without a specific regulatory mandate, whose disclosure would cause significant harm. Includes: donor and gift records, strategic plans, vendor contracts, personnel information without Restricted identifiers, and information covered by NDA.	Contractual obligations, reputational risk, competitive harm	Do NOT enter into any AI tool without explicit ITS authorization for the specific use case.
Tier 3: Internal Use	Non-sensitive internal information not intended for public release. Includes: procedures and manuals, internal org charts, intranet content, project reports, meeting notes, and network documentation. Default	Moderate reputational and operational risk if disclosed externally	May be entered into enterprise-approved AI tools only. Not into consumer or personal-account tools.

	classification for all unclassified data.		
Tier 4: Public	Information approved for public release. Includes: website content, press releases, published reports, marketing materials, and public event announcements.	No confidentiality restrictions	May be entered into approved AI tools.

6.1 Handling an Accidental Data Input

If you realize you have entered Tier 1 Restricted or Tier 2 Confidential data into an AI tool, take the following steps immediately:

5. Stop using the tool for the current session.
6. Document what data was entered, into which tool, and approximately when.
7. Report the incident to the ITS Helpdesk at helpdesk@morehouse.edu within one business day.
8. Do not attempt to delete the input yourself or assume the data was not retained by the tool.

Accidental inputs reported promptly and in good faith will be treated as incidents requiring remediation, not as intentional policy violations. Failure to report is treated as a separate and more serious matter.

7. Prohibited Uses

The following uses are prohibited for all staff, regardless of the tool or data involved.

7.1 Using Unapproved Tools for College Work

You may not use any AI tool not on the current approved list to conduct College business, process College data, or produce outputs that will be used in your official capacity. This includes using free consumer AI tools via a personal account for tasks involving College information, even if the information appears low-risk.

7.2 Entering Tier 1 Restricted or Tier 2 Confidential Data

Entering Tier 1 Restricted data into any AI tool is prohibited under all circumstances. Entering Tier 2 Confidential data into any AI tool without specific ITS authorization is also prohibited. This includes entering information about identifiable students, employees, donors, or patients, even in summary or partial form. If you are unsure whether the data you are working with is Tier 1 or Tier 2, treat it as Tier 1 and contact ITS before proceeding.

7.3 Relying on AI for High-Stakes Decisions Without Human Review

You may not use AI output as the sole or primary basis for decisions in the following categories without documented human review and approval by an authorized decision-maker:

- Student admissions, academic standing, financial aid eligibility, or conduct matters
- Hiring, performance evaluation, promotion, or termination of employees
- Financial approvals, procurement decisions, or contract terms
- Legal determinations or interpretations of College policy
- Any decision that creates a legal obligation for the College

AI tools may assist in preparing information for these decisions, but the decision itself must be made by a qualified human being who has independently reviewed the relevant facts.

These restrictions apply to administrative, operational, and institutional decisions and do not supersede faculty authority in academic evaluation, which is addressed in the Academic AI Guidelines.

7.4 Presenting AI Output as Original Work Without Disclosure

Staff may not submit AI-generated content as their own original analysis, research, or professional judgment in contexts where the distinction matters, such as grant applications, board reports, accreditation documentation, or formal evaluations. Disclosing AI assistance in these contexts is required.

7.5 Using AI to Circumvent Policy or Oversight

You may not use AI tools to circumvent approval processes, generate or alter documentation to misrepresent facts, or automate actions that would otherwise require supervisor or committee approval.

8. Best Practices for Responsible AI Use

The following practices will help you get the most value from AI tools while protecting the College and the people it serves.

8.1 Always Review AI Output Before Using It

AI tools produce text with confidence regardless of accuracy. Common errors include fabricated statistics, incorrect attributions, outdated information, and subtle factual distortions. Before using AI-generated content in any official capacity, read it carefully, verify specific claims against authoritative sources, and correct any errors. If you cannot verify a claim, remove it.

8.2 Be Specific in Your Prompts

The quality of AI output is directly related to the quality of your instructions. Vague prompts produce generic output. Specific prompts that include relevant context, the intended audience, and the desired format produce more useful results. You should still review and revise the output, but a well-constructed prompt reduces the need for revisions.

8.3 Do Not Share Your AI Account Credentials

Your enterprise AI tool accounts are provisioned for your individual use and are tied to your institutional identity. Do not share login credentials with colleagues, and do not use another

person's credentials to access AI tools. Each user must access tools through their own College account.

8.4 Think Before You Paste

Before copying content from any document into an AI tool, ask yourself whether that content contains sensitive information. This is especially relevant when summarizing meeting notes, drafting responses to complaints or inquiries, or processing documents from other departments. If the document contains names, ID numbers, financial details, or health information, do not paste it into an AI tool.

8.5 Keep a Record When It Matters

If you use AI assistance to produce a document, report, or communication that becomes part of an official College record or that informs a significant decision, note in your own records that AI was used and what tool was used. This supports transparency and accountability and protects you if questions arise later about how the work was produced.

8.6 Stay Current

The AI landscape is changing quickly. New tools become available, approved tools change their features and data practices, and policy requirements evolve. Check the ITS intranet page periodically for updates to the approved tool list and these guidelines. ITS will offer guidance sessions and training; participation is encouraged.

9. Roles and Responsibilities

Role	Responsibilities Related to AI Use
All Staff	Follow these guidelines and the AI Security and Risk Policy. Complete any required AI training. Report incidents promptly. Use only approved tools.
Supervisors and Department Heads	Set department-level expectations for AI disclosure and use. Ensure direct reports complete required training. Report suspected policy violations to ITS.
Information Technology Services (ITS)	Maintain the approved tool list. Conduct tool evaluations. Provide guidance and training. Manage AI-related incidents. Administer these guidelines. Contact: helpdesk@morehouse.edu
AI Governance Committee	Co-chaired by the CIO and Provost. Oversees AI policy development, reviews the AI Security and Risk Policy, and advises the President and Cabinet on institutional AI strategy.
Office of General Counsel	Advises on legal and regulatory compliance related to AI use. Consult for questions involving FERPA, HIPAA, contracts, or intellectual property.

10. Incident Reporting and Consequences

10.1 Reporting a Potential Violation

If you believe you have violated these guidelines, or if you observe another staff member doing so, report it to ITS as soon as possible. Contact the ITS Helpdesk at helpdesk@morehouse.edu or submit a ticket through the Service Portal.

Good-faith reports of accidental violations will be treated as opportunities for remediation and education. The College's priority, in most cases, is to address any data risk, resolve the issue, and prevent recurrence. Prompt reporting is the single most important factor in minimizing harm from an accidental incident. Incident handling and escalation processes align with the College's broader Incident Response and Information Security policies.

10.2 Consequences of Policy Violations

Intentional or repeated violations of these guidelines may result in disciplinary action, up to and including termination of employment, in accordance with applicable Human Resources policies. Violations that result in a data breach, regulatory violation, or legal liability for the College may also carry external consequences, including personal legal liability in serious cases.

Misuse of AI tools that compromise student data is taken seriously, given the College's obligations under FERPA and its duty of care to students.

11. Quick Reference Checklist

Use this checklist before and after using any AI tool for College work. A "No" answer to any question means you should stop and seek guidance before proceeding.

Question	Yes	No
Is the tool I am using on the ITS-approved tool list?		
Am I accessing the tool through my College account (not a personal account)?		
Have I confirmed the content I am entering contains no Tier 1 Restricted or Tier 2 Confidential data?		
Have I reviewed the AI output and verified any factual claims before using it?		
If this output will inform a high-stakes decision, has a qualified human being reviewed and approved it?		
If disclosure of AI use is required in this context, have I documented that appropriately?		

12. Document Management

Field	Details

Document Owner	Vice President and Chief Information Officer, Morehouse College
Maintained By	Information Technology Services (ITS)
Review Cycle	Annual, or as needed following significant changes in AI technology applicable law, or institutional policy
Current Version	1.0
Effective Date	April 2026
Next Scheduled Review	TBD
Questions / Contact	Servicedesk.morehouse.edu
Related Documents	Morehouse College AI Security and Risk Policy; Guidelines for the Academic Use of Generative AI; Data Governance Policy; Acceptable Use Policy