Reference Guide to UTech Policies Governing AI Use and Data Security

1. A Foundational Approach

Case Western Reserve University (CWRU) supports the responsible, innovative, and ethical use of Artificial Intelligence (AI) tools, including generative AI models, agentic AI systems, and emerging AI-enabled technologies, to advance learning, teaching, scholarship, research, and administrative operations.

Rather than treating artificial intelligence in isolation, CWRU's governance framework leverages established institutional policies to guide AI adoption. The University's existing information security posture establishes clear boundaries for data handling:

- The policy on Internal Use Only Data mandates that *"If cloud storage will be used, only approved cloud based services are authorized for storage of CWRU Internal Use Only information."*
- The policy on Restricted Use Data imposes even stricter physical, technical, and administrative controls.

Consequently, whenever members of the university community utilize AI tools to process, analyze, generate, or interact with university information, they must use CWRU-approved AI platforms that align directly with the appropriate data classification level. All AI activities must comply with applicable federal, state, local, and international laws, as well as overarching university regulations such as the Acceptable Use Policy. Ultimately, each user is responsible for all work and academic products co-created with AI, remembering to keep the human in the loop.

---

2. Scope

University data policy applies to all individuals and entities interacting with CWRU data, systems, or academic and operational environments, including:

- All members of the CWRU community (faculty, staff, postdocs, and students).

- Volunteers, visiting scholars, and contractors or third-party personnel operating on behalf of the University.
- Any individual or automated system granted access to CWRU information assets or networks.

---

3. Definitions

- **Generative AI:** A class of artificial intelligence systems designed to process user questions, prompts, files, and multi-modal inputs (e.g., text, code, images, audio, video) to produce synthetic, human-like outputs (e.g., written documents, analytical summaries, software scripts, or artistic designs). Generative AI includes both standalone web applications and capabilities embedded directly within enterprise productivity suites.
- **Agentic AI:** Autonomous or semi-autonomous AI systems capable of executing multi-step goals, initiating actions, making decisions, querying APIs, running workflows, or interacting across disparate software platforms on behalf of a user or system with limited or no real-time human intervention.
- **Data Classifications:**
  - **Public Data:** Information intended for public distribution or freely available without restriction.
  - **Internal Use Only Data:** Information intended for internal university operations whose unauthorized disclosure could cause moderate operational, financial, or reputational impact (includes standard student educational records under FERPA).
  - **Restricted Data:** Highly sensitive information strictly regulated by law, contract, or university mandate, requiring the highest level of security controls (e.g., HIPAA-covered health records, financial account numbers, export-controlled data, and restricted research data).

---

4. Data Classification Policy Implications for AI Usage

4.1 Privacy and Data Protection

All data entered into, retrieved by, or shared with AI systems, including data utilized for prompt engineering, model tuning, retraining, grounding, or automated evaluation, must strictly adhere to CWRU information security and privacy standards.

1. **Non-Approved / Consumer AI Services:** Public, consumer, or personal AI accounts (such as free web tiers or personal subscriptions) may **only** interact with publicly available data. Entering internal use only or restricted institutional information into personal or unapproved AI tools is strictly prohibited.
2. **Prohibited Sensitive Data on Unapproved Platforms:** Under no circumstances internal use only or restricted data, such as the examples below, be entered into, retained by, or used to fine-tune non-approved AI services:

    - Student education records, evaluations, admissions materials, or personally identifiable information (PII) governed by the Family Educational Rights and Privacy Act (FERPA).
    - Confidential personnel, payroll, or human resources records.
    - Health, patient, medical, or clinical research data subject to institutional, state, or federal privacy regulations (e.g., HIPAA, IRB requirements).
    - Financial, banking, donor, or payment card information governed by GLBA or PCI-DSS.
    - Proprietary institutional assets, unpublished research, patent disclosures, pre-publication scholarship, legal communications, or non-public strategic plans.

3. **Agentic Data Guardrails:** Specific technical safeguards must be configured before deploying agentic AI to prevent agents from inferring, caching, persisting, or transmitting sensitive university data beyond their authorized scope of execution.

4.2 Security, System Controls, and Approved University AI Services

Use of generative and agentic AI for university administrative work, instruction, and operational workflows must occur within secure, institutionally managed, and contractually protected environments.

CWRU provides vetted platforms where vendor contracts stipulate robust privacy protections, auditing capabilities, and strict assurances that institutional prompts and uploaded data are not used to train external foundational models. Because security risks escalate when tools possess execution privileges or access sensitive data stores, higher-tier services require specific training, terms of service agreements, or license allocations.

The table below outlines current university-approved AI services, their cleared data classification levels, and access prerequisites:

Service	Authorized Data Classification Level	Additional Requirements for Use
Gemini Enterprise and Gemini Enterprise Notebook (Standard Version)	Public Data & Internal Use Only *(FERPA data classified as internal use only allowed)*	Completion of university training and acceptance of Terms of Service
Gemini Enterprise and Gemini Enterprise Notebook (Restricted Data Version; availability to be announced)	Restricted Data	Explicit administrative approvals, completion of specialized training, acceptance of Terms of Service, compliance documentation, and allocated paid licensing
Gemini for Google Workspace and Gemini Notebook	Public Data & Internal Use Only	Log in with CWRU username and passphrase
Microsoft Copilot	Public Data & Internal Use Only	Log in with CWRU username and passphrase
Claude Education Plan (license purchased from CWRU)	Public Data & Internal Use Only	Administrative approval, completion of training, acceptance of Terms of

		Service, and paid licensing
ChatGPT Business Plan (license purchased from CWRU)	Public Data & Internal Use Only	Administrative approval, completion of training, acceptance of Terms of Service, and paid licensing
CWRU AI	Public Data & Internal Use Only	Acceptance of Terms of Service

Note: For the latest roster of approved tools, consultation resources, and service request links, refer to the CWRU AI Tools and Resources Portal.

4.3 Governance for New AI Procurement and Internal Development

To maintain institutional compliance and technical integrity:

- Any new commercial or third-party AI platform, tool, or plugin purchased with university funds (including department budgets, grant funds, or p-cards) must undergo formal review and approval by the **University AI Governance Committee** and UTech Information Security prior to procurement.
- Any internally developed AI systems, custom large language models, retrieval-augmented generation (RAG) pipelines, or custom autonomous agents built by university units or researchers for operational or broad campus use must be submitted to the AI Governance Committee for architectural, privacy, and risk assessment.

4.4 Agentic AI Deployment and Safeguards

Agentic AI systems introduce distinct operational and security challenges because they interact dynamically with external APIs, databases, filesystems, and execution environments.

- **Prohibition on Unvetted Deployment:** Only CWRU-approved agentic services can be used with university data and systems. Any other agentic AI platforms that initiate workflows, execute transactions, alter system states, connect to university enterprise infrastructure, or take other actions that risk university data or infrastructure may not be enabled or deployed without explicit institutional security review and approval.

- **Mandatory Safeguards:** All approved agentic implementations must incorporate:
  - Strict identity and access management (IAM) using principle-of-least-privilege credentials.
  - Comprehensive logging and audit trails capturing agent actions, queries, tool calls, and decisions.
  - Human-in-the-loop (HITL) checkpoints or hard execution boundaries for irreversible, high-impact, or sensitive operations.
- **Ancillary Risk:** Users must exercise caution with ancillary tools (e.g., browser extensions, personal plugins, unmanaged code execution environments). Pairing an institutional AI model with unvetted ancillary extensions voids institutional protections and creates substantial data exposure risks.

4.5 Compliance, Licensing, and Legal Obligations

All AI utilization must respect applicable statutory, regulatory, and contractual obligations:

- Users must abide by vendor licensing agreements, terms of service, and acceptable use guidelines governing each approved platform.
- Outputs must not infringe upon intellectual property, patent rights, trademarks, or copyrights.
- The individual configuring, prompting, or deploying an AI tool remains personally and institutionally responsible for verifying the accuracy, integrity, legality, and appropriateness of all outputs and automated actions. AI cannot serve as an authorized legal signatory, official certifier, or primary accountable actor.

4.6 Intellectual Property and Data Ownership

- **Institutional Environments:** Content, data, analytical code, and intellectual property generated within CWRU-licensed AI environments remain subject to existing university policies regarding data ownership and copyright. Prompts and generated outputs within approved institutional platforms do not become the property of third-party model providers.
- **Rights Retention:** Consistent with university intellectual property policies, faculty, researchers, and students retain appropriate rights to their scholarship, creative works, and course deliverables created within institutional tools.
- **Unlicensed Platforms:** Utilizing unapproved or public consumer AI platforms compromises these protections, possibly including the loss of intellectual

property rights; commercial terms on consumer platforms frequently claim broad licenses to user inputs and outputs.

---

5. Community Accountability

Every member of the CWRU community bears personal responsibility for safeguarding university information assets:

4. **Oversight:** Community members must actively oversee AI-assisted outputs, review generated code for vulnerabilities, and inspect text or analysis for hallucinations, inaccuracies, or bias before utilizing it in institutional decisions. Users should cross-reference their outputs with primary sources and ensure their work is peer-reviewed.
5. **Delegation to Agents:** Users who configure or delegate tasks to autonomous agentic workflows remain directly answerable for the system actions, API calls, and downstream impacts executed under their credentials.
6. **Instructional Transparency**: Faculty and instructors are strongly recommended to explicitly outline permitted and prohibited uses of AI tools within their course syllabi to provide clear academic integrity expectations for students. Correspondingly, students must adhere to these course-specific guidelines, and appropriately disclose and cite permitted AI assistance,

---

6. Policy Enforcement and Sanctions

Compliance with this policy is critical to safeguarding the university's legal standing, data confidentiality, and technical infrastructure.

- **Standard Disciplinary Procedures:** Violations will be handled through established university disciplinary processes appropriate to the individual's role (faculty handbook procedures, staff corrective action, or the student code of conduct).
- **Sanctions:** Sanctions may include mandatory retraining, revocation of AI service access, administrative suspension of university computing privileges, or, in severe cases, termination of employment or academic expulsion.
- **Immediate Administrative Action:** The University reserves the right to immediately suspend, block, or revoke access to any AI platform, service

integration, account, or agentic workflow without prior notice when necessary to protect the security, integrity, or legal liability of CWRU computing resources.

---

7. Exceptions and Specialized Authorizations

Exceptions to this policy may be granted under narrow circumstances where academic research, pedagogical experimentation, or specialized operational requirements necessitate alternative configurations.

- **Submission:** Written requests for exceptions must be submitted to the Chief Information Officer (CIO) detailing the technical architecture, data handling safeguards, risk mitigation strategies, and institutional justification. To get started with the process, schedule an AI consultation with UTech.
- **Evaluation:** The CIO evaluates exception requests in coordination with the University Risk Officer, Information Security, and the Office of the General Counsel as appropriate.

---

8. Applicable University Policies and References

This policy operates in conjunction with related CWRU governance, compliance, and security frameworks:

- Acceptable Use of Information Technology Policy (AUP)
- Controls for Protecting Internal Use Information Systems
- Controls for Protecting Restricted Information Systems
- Information Types and Data Sensitivity Classifications
- Case Western Reserve University Copyright Compliance Policy
- CWRU AI Tools and Resources Directory