

## Artificial Intelligence Acceptable Use & FERPA Compliance Policy

### Overview

This policy outlines the permissible use of artificial intelligence (AI) tools and systems within Vermont Law and Graduate School (VLGS), emphasizing compliance with the Family Educational Rights and Privacy Act (FERPA). It applies to all faculty, staff, contractors, and third-party vendors who use or manage AI technologies in any academic or administrative context.

### Definitions

- **First-Party AI Services (CoPilot):** Artificial intelligence applications or services that are operated internally. At VLGS, Microsoft CoPilot is a first-party service where all data stays within the VLGS tenant without feeding back to the main commercial model.
- **Third-Party AI Tools (AI Tools):** Artificial intelligence applications or services developed and operated by external vendors, often hosted in the cloud, that process data and deliver outputs such as text, images, or predictions. (i.e. ChatGPT, Claude, LLaMA).
- **Family Educational Rights and Privacy Act (FERPA):** A federal law that protects the privacy of student education records. It grants students certain rights over their records and restricts access and disclosure of those records without consent, except under specific allowable conditions.
- **Personally Identifiable Information (PII):** Any data that can be used to identify a student or individual, including but not limited to:
  - Names
  - Addresses
  - Social Security Number
  - Birthdate
  - Student ID numbers
  - Grades
  - Other education records covered under FERPA.
- **Other Sensitive Information:** Individual or institutional information including:
  - Giving history
  - Family details
  - Financial information
  - Medical history or current conditions

### Use of AI with Student Data

- AI Tools must not process, analyze, or access education records containing PII or other sensitive information unless:
  - There is a documented legitimate educational interest, and
  - Use complies with FERPA exceptions or written student consent has been obtained.
    - Co-Pilot, included in the VLGS licensed version, complies with FERPA.
    - Open-source AI Tools does not.
- Data used to train or operate AI Tools must be de-identified, or anonymized, unless explicit FERPA-compliant permissions are in place.
- Before inputting any data into a generative AI Tool, ensure that it does not include PII. This includes data that identifies a student or individual and is protected under FERPA, institutional privacy standards, or other applicable regulations or agreements. Improper use may violate federal regulations or institutional policies.

### **Third-Party AI Tools**

- All third-party AI tools must be vetted through the IT Department for FERPA and PII compliance. The following AI Tools have been evaluated:
  - CoPilot – compliant
  - ChatGPT – not compliant
  - Claude – not compliant
  - LLaMA – not compliant
- Contracts with vendors must include:
  - FERPA-aligned data handling provisions
  - Prohibitions on reusing institutional data to train external AI models
  - Right-to-audit clauses for data security

### **Transparency and Notification**

- Employees must be notified when AI Tools are used by the institution in ways that may impact them—such as in disciplinary, performance evaluation, or hiring decisions.
- When AI Tools are involved in decision-making, a human review must be available upon request.

### **Acceptable Use**

Employees may use AI tools to support their professional responsibilities, including communication and administrative tasks. Use must align with institutional policies, applicable laws, and the school's mission.

AI generated content must be reviewed for accuracy, appropriateness, and compliance with school policies by the individual who generated it prior to use or distribution.

Employees must not use AI Tools to:

- Generate or disseminate misleading, discriminatory, or harmful content
- Replace critical human judgment in areas such as student assessment, disciplinary actions, or legal decisions
- Input or share records containing personally identifiable information (PII) or other sensitive institutional data with AI platforms, unless explicitly authorized and compliant with data privacy regulations and institutional policy

Use of AI must be disclosed when doing so is appropriate and must not compromise data privacy, security, or the educational mission of the institution.

### **Security and Access**

- Access to AI tools handling student data requires:
  - Multi-factor authentication (MFA)
  - Role-based access controls
  - Regular auditing and logging of system activity
- Users are required to comply with VLGS privacy and security guidelines when entering any information into AI tools.

### **Oversight and Policy Review**

- The VP of Operations will oversee the implementation and yearly review of this policy.
- Employee violations of this policy may result in disciplinary action consistent with VLGS personnel and academic policies, including those outlined in the Faculty and Staff Handbooks.
- Contractor or third-party vendors that fail to comply with VLGS data protection policies could result in revocation of system access and/or termination of contracts.