Policy Brief

April 2025

For more information, visit www.heatherdorrell.com

Safeguarding Student Privacy in the Age of AI

Navigating the Challenges of Large Language Models in Higher Education

EXECUTIVE SUMMARY

The rapid adoption of Large Language Models (LLMs) highlights privacy and security concerns in higher education.

- **Key Takeaways:** LLMs use vast amounts of student data for machine learning in order to operate. This raises concerns for data privacy, security, and compliance.
- **Faculty and Staff** need specialized training on AI data privacy risk practices.
- **Regulations** must be modified and implemented to provide clear governance regarding the use of LLMs in higher education settings.

Policy Challenges Facing Universities

Data Governance Gaps

Many institutions lack clear AI-specific privacy policies.

Compliance Uncertainty

Universities struggle to ensure AI tools meet FERPA & GDPR standards.

Limited Faculty Training

Most faculty are not trained in AI privacy risks.

Privacy & Security Challenges

As universities integrate AI-powered tools, student privacy and data security risks increase.

Unclear Data Ownership

Who controls student data processed by LLMs?

Lack of Transparency

Are students aware their data is being used for AI training?

Regulatory Compliance

How will universities align regulations with FERPA, GDPR, and institutional policies?

Recommended Actions for Leaders

1. **Establish Specific AI Data Governance Policies**
   - Require AI vendors to comply to FERPA & GDPR
   - Define data collection, usage, and retention
2. **Implement Faculty & Staff AI Privacy Training**
   - Mandatory workshops on AI-driven privacy risks
   - Develop guidelines for responsible AI use and enforcement procedures
3. **Introduce Transparency & Opt-Out Mechanisms**
   - Inform students when AI tools collect their data
   - Allow students to opt-out and provide alternative assignments/assessments