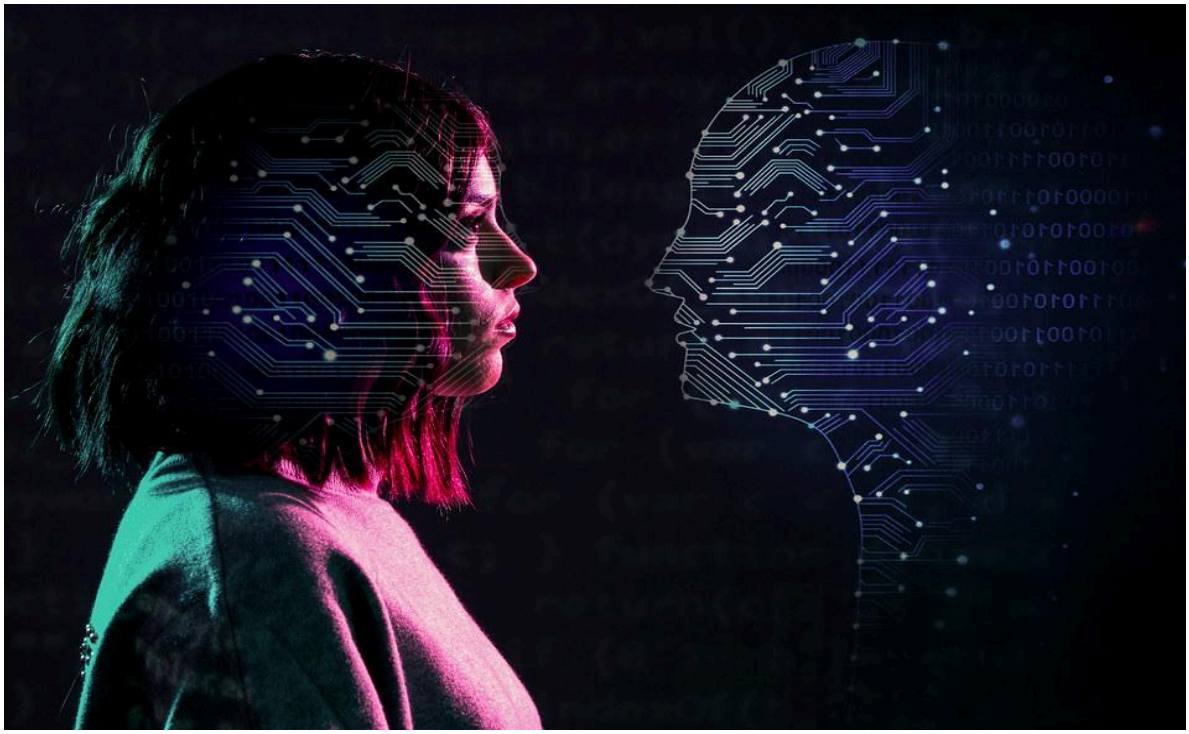
Technology, Learning Systems, and Culture

The AI Balancing Act: Safeguarding Privacy, Compliance, and Ethics in Higher Education

For Concerned Higher Education Administrators, Policy Makers, IT Leaders, and Faculty Governance Committees



Introduction

Generative AI is transforming how universities operate—but at what cost? While tools powered by large language models (LLMs) offer efficiencies, they also introduce complex risks related to student privacy, institutional compliance, and academic equity. Despite this, faculty often receive little training or guidance on how to use these technologies safely or ethically. As institutions race to implement AI-driven solutions, the absence of clear governance frameworks and risk mitigation strategies leaves students vulnerable to data misuse and systemic harm.This policy brief explores the most pressing data and privacy risks tied to LLMs in higher education, identified through a literature review of peer-reviewed studies from 2021–2025. Findings are synthesized into an "AI Risks Radar" framework for use by academic leaders and policymakers.

> "Data protection is not simply a technical issue—it is a matter of educational justice."
>
> Holmes et al. (2021)

Background & Context

Since the public release of tools like ChatGPT in 2022, generative AI has rapidly entered university environments through both formal and informal channels. Students use AI for writing assistance and exam prep. Faculty experiment with AI to grade or create content. Meanwhile, third-party vendors integrate LLMs into learning management systems with minimal oversight. Yet, few institutions have comprehensive AI governance frameworks in place.

Current legislation offers some protections, but many LLM applications fall into gray zones. The scale of institutional unpreparedness became evident in surveys conducted across U.S. and European universities between 2022 and 2024 (Holmes et al., 2021; Moore & Lookadoo, 2024).

This policy brief synthesizes peer-reviewed research and organizational reports, including comparative policy analyses, survey data from higher education staff, and risk modeling tools.

Key Findings and Risks from AI Use in Higher Education

Opaque Data Practices and Vendor Dependencies: Most LLMs are developed by third-party vendors. Universities often lack visibility into how student data is collected, used, and stored, raising FERPA and GDPR compliance issues *(Neel & Chang, 2024).*

Surveillance and Algorithmic Bias: AI tools may perpetuate bias, track behavior without consent, and exploit marginalized student data *(Gupta & Treviranus, 2020;Zuboff, 2019).*

Lack of Institutional Policy and Oversight: Only 32% of universities have formal AI policies, relying on individual faculty members and IT departments to manage the use of GenAI security in isolation *(Moore & Lookadoo, 2024; Ulven & Wangen, 2021).*

Limited Faculty Training: Faculty often lack awareness of data risks, inadvertently exposing student information to breaches or bias *(Chen et al.; Das et al., 2024).*

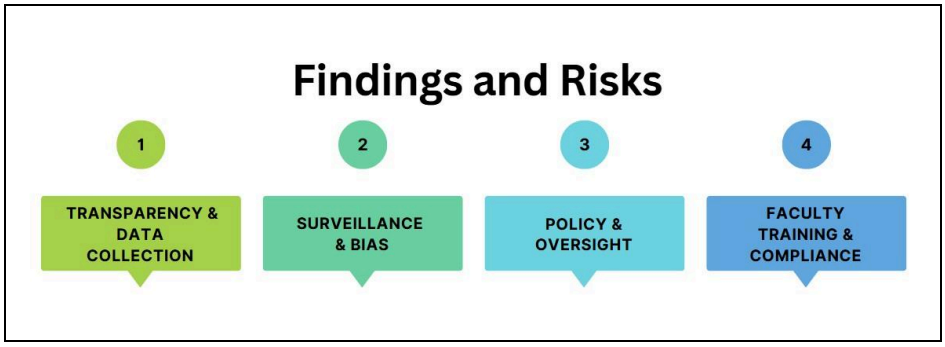


Figure 1: Key Findings and Risks from AI Use in Higher Education

AI Risks Radar: Eight Critical Domains

The eight critical risk domains of the AI Risks Radar highlight key vulnerabilities in student data privacy, security, and governance within higher education. From algorithmic bias and inequitable access to opaque data practices, compliance challenges, and limited autonomy in AI-driven systems, these risks underscore the urgent need for transparent, student-centered AI policies that uphold legal and ethical standards.

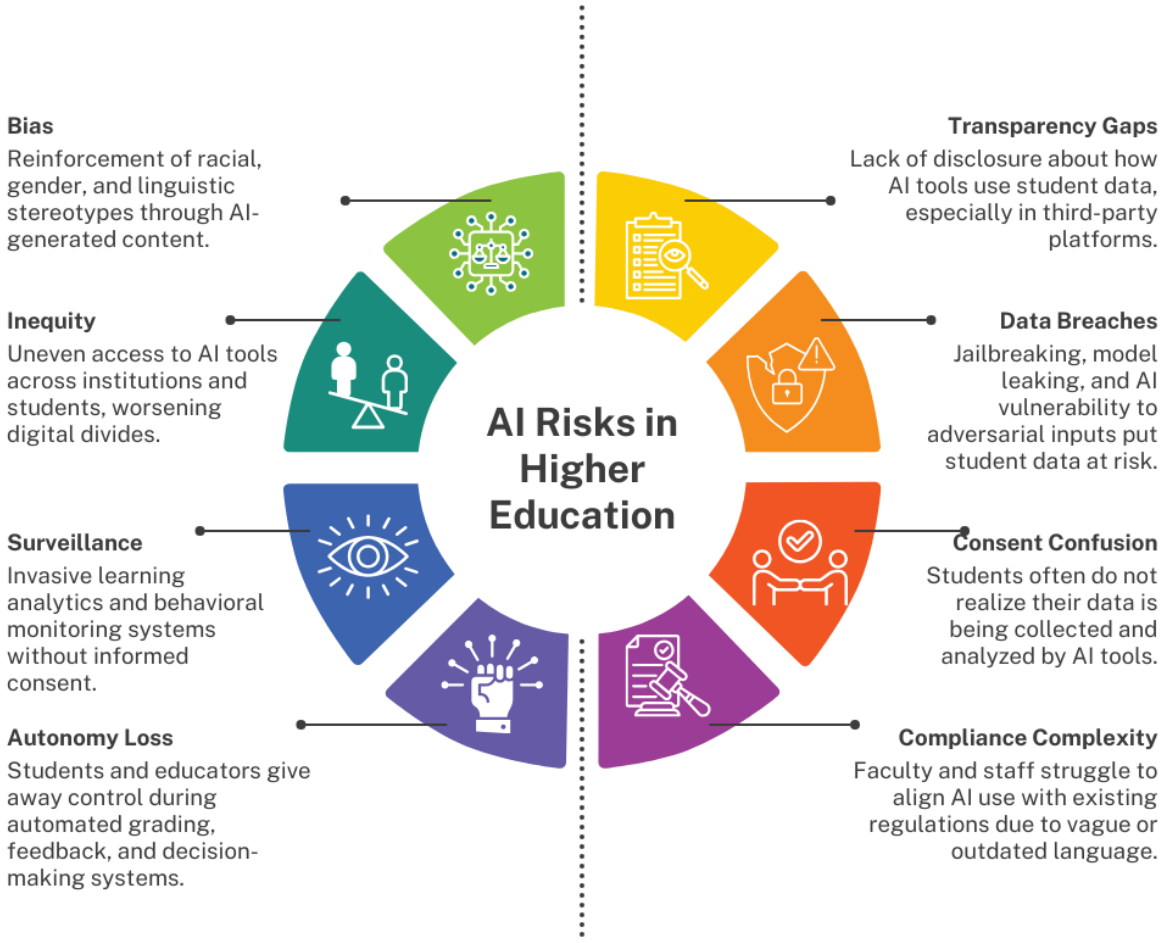


Figure 2: Eight Categories of AI-Related Risk in Higher Education

Policy Implications

University administrators and policymakers must urgently address these vulnerabilities. Proactive governance is essential to mitigating risk. Policies must balance innovation with student protections, legal compliance, and institutional ethics.

Without interventions, risks include:

- Violating federal or international data policy protection laws.
- Losing student, faculty, and public trust due to AI-related privacy scandals.
- Exacerbating educational inequality through algorithmic bias or exclusion.

Recommendations

As generative AI becomes embedded in higher education, institutions must adopt proactive strategies to safeguard student data, ensure legal compliance, and build trust. The following recommendations provide a structured approach to managing AI-related risks through governance, cybersecurity, and inclusive policy design.

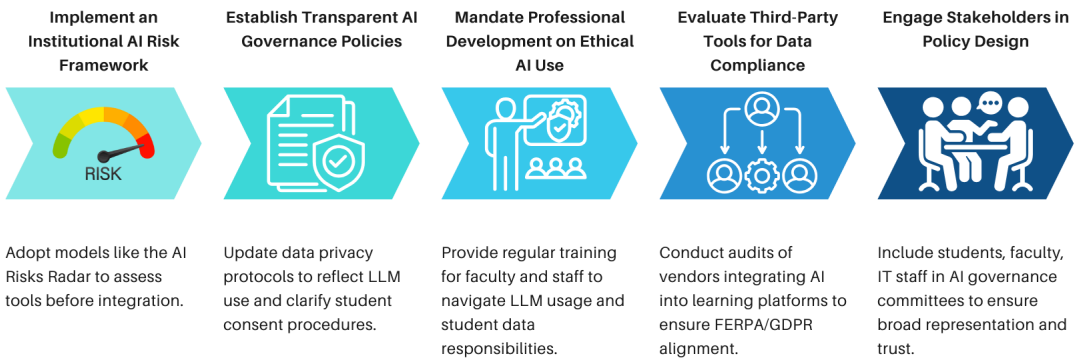


Figure 3: Five Recommendations for AI Risk Management

Recommendation 1: Implement an Institutional AI Risk Framework

- Include an interactive and mandatory AI Risk assessment and review.
- Conduct annual audits to identify compliance gaps and monitor emerging risks (Data Quality Campaign, 2023).

Recommendation 2: Establish Transparent AI Governance Policies

- Update privacy protocols to reflect LLM use and clarify student consent procedures.
- Clearly define data parameters by identifying what student data AI tools can access, limiting storage duration, and enforcing deletion policies (Das et al., 2004).
- Include opt-out policies and allow students to choose whether their data is used and offer non-AI alternatives.

Recommendation 3: Mandate Professional Development on Ethical AI Use

- Provide regular training for faculty and staff to navigate LLM usage and student data responsibilities.
- Build awareness around privacy, ethics, and safe AI use by employing faculty and student AI literacy programs (Chen et al., 2025).

Recommendation 4: Evaluate Third-Party Tools for Data Compliance

- Conduct audits of vendors integrating AI into learning platforms to ensure FERPA and GDPR compliance.
- Require clear documentation on data use, bias mitigation, and security to provide for transparency and vendor accountability (Tzmias & Demetriadis, 2021).
- Use encryption, multi-factor authentication, differential privacy, and real time monitoring cybersecurity measures (Neel & Chang, 2024).

Recommendation 5: Engage Stakeholders in Policy Design

- Include students, faculty, and IT staff in AI governance committees to ensure broad representation and trust.

Conclusion

To safeguard student data and uphold ethical standards, university leaders must act now to update policies, implement targeted training, and establish clear accountability for AI use. By recognizing the risks of introducing LLMs into the higher education ecosystem and taking steps recommended in this policy brief, administrators, policy makers, IT Leaders, and faculty governance leaders will make positive progress toward safeguarding student data and upholding ethical standards in the future.

References

Chen, K.; Tallant, A.C.; Selig, I. Exploring generative AI literacy in higher education: Student adoption, interaction, evaluation, and ethical perceptions. *Inf. Learn. Sci.* 2024.

Das, B. C., Amini, M. H., & Wu, Y. (2024). *Security and privacy challenges of large language models: A survey*. *Journal of the ACM, 37*(4), Article 111.

Data Quality Campaign. (2023). *DATA 101: A briefing book for policymakers on education to workforce data*. https://dataqualitycampaign.org/resource/data-101-briefing-book-policymakers/

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to threatgpt: Impact of generative AI in cybersecurity and privacy. IEEE Access.

Holmes, W., & Porayska-Pomsta, K. (Eds.). (2023). *The ethics of artificial intelligence in education: Practices, challenges, and debates*. Routledge. https://doi-org.proxy1.library.virginia.edu/10.4324/9780429329067

Moore, S., & Lookadoo, K. (2024). Communicating Clear Guidance: Advice for Generative AI Policy Development in Higher Education. Business and Professional Communication Quarterly, 87(4), 610-629. https://doi.org/10.1177/23294906241254786

Neel, S., & Chang, P. (2023). Privacy issues in large language models: A survey. *arXiv preprint arXiv:2312.06717*.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.