To:
U.S. Department of Education, Student Privacy Policy Office (SPPO) and Office for Civil Rights (OCR); with coordination from the Office of Postsecondary Education (OPE)
From:
Sherlock Jr. Langevine
Date:
January 20, 2026
Subject:
Strengthening Federal Requirements for AI-Related Student Data Privacy and Governance in Higher Education

Decision Requested

Direct the U.S. Department of Education (ED) to issue binding guidance and funding conditions that require universities and educational institutions to adopt strengthened student data privacy governance for AI-related systems. This should include:

1. **Standardized data governance frameworks** that explicitly limit collection, use, and sharing of student data for AI purposes beyond core educational functions.
2. **Mandatory transparency and reporting** to students, parents, and regulators about what data is used, how it is processed by AI systems, and with whom it is shared.
3. **Independent third-party audits** of AI data practices at institutions receiving federal funds to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and emerging AI privacy best practices.
4. **Prohibit secondary use and monetization** of student data (including de-identified or derived data such as engagement scores) for non-educational purposes without affirmative, opt-in consent and strong contractual limits on vendor reuse.

Executive Summary

- A key gap is that de-identified and derived student data can be repurposed for product development, model training, or commercial uses that students did not reasonably expect and cannot meaningfully audit.
- Student data privacy in the context of AI adoption on campuses and in school systems remains inconsistent and under-governed by clear federal frameworks. Education technology and AI tools increasingly integrate sensitive information that is not always visible to students or protected beyond existing FERPA compliance.
- Recent news shows that student data breaches continue to occur, underscoring the vulnerability of current systems to unauthorized access and highlighting the absence of clear nationwide governance expectations.
- Institutional data governance capacity remains uneven, and many schools lack basic governance structures to protect AI-related data usage.

- Current federal guidance from ED affirms principles for responsible AI use but stops short of requirements specific to student data lifecycle governance, consent disclosures, and external sharing.
- Strengthened requirements can be implemented through federal guidance tied to education funding eligibility and periodic audits, closing gaps in transparency and accountability while preserving beneficial uses of AI in education.

Context and Problem

AI and data-driven educational technologies are rapidly adopted in higher education to support learning management, virtual classrooms, and predictive analytics. However:

Lack of Clear National Standards

Federal guidance on AI in education affirms responsible use principles but does not establish clear, enforceable frameworks for how student data may be collected, processed, retained, or shared by AI systems.

Data Governance Gaps

Many districts and institutions lack formal privacy policies or clearly designated governance roles for managing student data used in AI systems. A report by the Consortium for School Networking finds insufficient policy infrastructure and training for key personnel.

Ongoing Breach Risks

Recent higher-education incidents show that universities are attractive targets precisely because student data and campus workflows are concentrated in a small number of enterprise and learning platforms. In 2025, Harvard University reported being targeted in a cyber extortion campaign linked to vulnerabilities in Oracle E-Business Suite, part of a broader wave in which attackers exfiltrated data and attempted to extort organizations running widely deployed enterprise systems. This pattern is directly relevant to higher education because many institutions run comparable “hub” systems for identity, HR, finance, student information, and learning infrastructure. When these systems are compromised, attackers can obtain both direct identifiers and sensitive inferred data created by analytics and AI-enabled workflows. The policy implication is that privacy governance cannot stop at “FERPA compliance” for records; it must require institution-wide vendor controls, logging, retention limits, and independent audits for any AI-related student data pipelines.

Increasing Complexity with AI

In higher education, learning management systems such as Canvas concentrate course content, messaging, grading, and third-party tool integrations in a single vendor platform. These systems generate detailed logs of student activity and engagement that can be used to infer

behavioral profiles or risk scores. Because this platform-derived telemetry is not always treated as part of a student's formal "education record," it can fall into a gray zone under FERPA, creating gaps in retention rules, secondary use limits, and accountability when data move to vendors or integrated tools.

Even when institutions do not "sell" identifiable student records, AI-era data practices can enable a quieter form of extraction: platform logs, engagement metrics, and other derived data can be retained, aggregated, and reused for product improvement or model development by vendors or downstream partners under broad contract terms. Because these data may be de-identified or treated as outside the core "education record," they can slip past the expectations and controls that govern traditional FERPA-protected records, leaving students with limited visibility into secondary use and limited leverage to opt out.

Policy Recommendations

1) Establish Mandatory Governance Frameworks

What:
Require institutions that receive federal education funds to implement formal student data governance frameworks that:

- Define roles and responsibilities for data stewardship, access control, and privacy compliance.
- Map all student data collection and AI system interactions.
- Set purpose limitation for AI and data use tied to core educational outcomes.

How:

- Use ED privacy and security technical assistance channels (PTAC) to publish a template governance framework.
- Tie compliance to access to Title IV federal funds and institutional eligibility.

Why:
Standardizing governance ensures all institutions have minimum practices to protect student data across AI systems.

2) Require Transparency and Student/Parent Reporting

What:
Develop a standard student/parent notification and consent protocol for AI systems that collect or process student data, including:

- What data is being collected

- How AI systems process or retain it
- Who has access to it and third parties involved
- Retention and deletion timelines

How:

- ED should issue regulatory guidance and templates for transparency statements; requiring institutions to publish these on official websites and student portals.
- Institutions should also file annual reports to ED on their AI systems and data practices.

Why:
Transparent reporting empowers students and families to understand and challenge how personal information is used.

3) Mandate Third-Party Audits of AI Data Practices

What:
Require institutions to commission independent audits of their AI-related data systems, focused on:

- FERPA compliance
- Data lifecycle security
- Unauthorized sharing practices
- Adherence to transparency disclosures

How:

- Set audit frequency (e.g., biennially for large universities, every three years for smaller institutions).
- Provide federal funding assistance or subsidized audit programs for institutions with limited resources.

Why:
Independent assessments provide accountability and early detection of non-compliance or privacy gaps before breaches occur.

Implementation Strategy

1. **ED Guidance Revision (0–6 months):**
   ED's Office for Civil Rights and PTAC update AI guidance to include mandatory governance, transparency, and audit requirements tied to federal fund eligibility.

2. **Model Policies and Templates (6–12 months):**
   Publish governance, reporting, and consent template documents for institutions.
3. **Capacity Building (12–24 months):**
   Run workshops and training for institutional privacy officers and leadership.
4. **Audit Program Rollout (24–36 months):**
   Begin audit cycles for early adopters and support implementation across systems.

Stakeholders

- **Students:** Gain clarity and control over how personal data is used and protected.
- **Universities:** Must implement stronger governance and reporting practices.
- **EdTech Vendors:** Must comply with institutional frameworks and transparency requirements.
- **Federal Regulators:** ED leads, with potential support from FTC for enforcement of unfair or deceptive practices.

Conclusion

Strengthening student data privacy governance for AI systems is an urgent national priority. Recent evidence shows data governance gaps, rising AI adoption in education, and continued breach risks. A coordinated federal framework that embeds governance requirements into funding eligibility, mandates transparency, and institutionalizes independent audits will protect students while enabling responsible educational innovation.

References

- U.S. Department of Education, Student Privacy Policy Office. (n.d.). Protecting student privacy. https://studentprivacy.ed.gov/
- U.S. Department of Education. (2025, May 2). U.S. Department of Education issues guidance on artificial intelligence use in schools, proposes additional supplemental priority (Press release). https://www.ed.gov/about/news/press-release/us-department-of-education-issues-guidance-artificial-intelligence-use-schools-proposes-additional-supplemental-priority
- Congressional Research Service. (2021, May 24). The Family Educational Rights and Privacy Act (FERPA): Legal issues (R46799). https://www.congress.gov/crs-product/R46799

- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
- National Institute of Standards and Technology. (2024). Artificial intelligence risk management framework: Generative AI profile (NIST AI 600-1). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
- Federal Trade Commission. (2022, August 11). Commercial surveillance and data security rulemaking. https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking
- Instructure. (n.d.). Product privacy | Policy. https://www.instructure.com/policies/product-privacy-policy
- Stanford University. (n.d.). Canvas data collection and usage. https://gocanvas.stanford.edu/about/canvas-data-collection-and-usage
- University of Phoenix. (2025). University of Phoenix data breach disclosure after Oracle hack. https://www.bleepingcomputer.com/news/security/university-of-phoenix-discloses-data-breach-after-oracle-hack/
- University of Pennsylvania & University of Phoenix. (2025). Penn and Phoenix universities disclose data breach after Oracle EBS hack. https://www.securityweek.com/penn-and-phoenix-universities-disclose-data-breach-after-oracle-hack/