Case Studies in AI:

Helping staff and students use AI in fair and privacy-protective ways

PUBLIC INTEREST PRIVACY CENTER

Challenges

- **AI efficacy**
  - Widespread puffery (or lies) from edtech providers
  - Lack of efficacy research
  - Misunderstandings about what AI can do
- **AI adoption**
  - AI is already being used in education
  - AI is being incorporated into existing edtech without notice
- **AI understanding**
  - Application of existing laws
  - Lack of awareness about AI/algorithmic harms
  - Lack of awareness of toolkits and other useful resources (and established experts over the past decade)
- **Old challenges**
  - In many ways, the biggest challenges–and the greatest solutions–related to AI in K-12 are preexisting challenges about the adoption and use of education technology.
- **New challenges**
  - Questions about using student PII to train algorithms (past, present, and future)

Our Privacy Law Toolbox

Family Educational Rights and Privacy Act (FERPA)	
High-Level Overview:	• Requires schools to protect the privacy of education records and to give parents (and eligible students) access to them.
Applicability to LEAs:	• Directly regulates LEA data governance and transparency
Key Provisions:	• **ACCESS**: Guarantees parents (& eligible students) access to education records • **PRIVACY**: Prevents unauthorized disclosure of education records without consent or very specific safeguards
Frequent LEA Concerns:	• LEAs often need expert assistance to navigate FERPA because many of its requirements exist not in the law itself, but are rather found in accompanying regulations, USED guidance documents, complaint letters, etc.

Protection of Pupil Rights Amendment (PPRA)	
High-Level Overview:	• Regulates certain data collection from students (mostly surveys) and requires schools to give parents access to instructional materials upon request.
Applicability to LEAs:	• Directly regulates LEAs
Key Provisions:	Requires schools to: • Notify parents and let them opt-in or opt-out of surveys, especially when asking about: 1. Political affiliations; 2. Mental and psychological problems potentially embarrassing to the student and his/her family; 3. Sex behavior and attitudes; 4. Illegal, anti-social, self-incriminating and demeaning behavior; 5. Critical appraisals of other individuals with whom respondents have close family relationships; 6. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; 7. Religious practices, affiliations, or beliefs of the student or student's parent; 8. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program.). • Notify parents when student personal information will be collected, used, or disclosed for marketing purposes • Notify parents when students are scheduled to participate in physical exams • Give parents access to instructional materials upon request
Frequent LEA Concerns:	• PPRA is less well-known than FERPA, so LEA staff may be unfamiliar with its requirements. • Sometimes limits LEA ability to do social-emotional learning (SEL), school climate, and student interest surveys without parent notice and consent.

Children's Online Privacy Protection Act (COPPA)	
High-Level Overview:	• Parental consent required before companies collect personal information from children under 13.
Applicability to LEAs:	• **Doesn't** directly regulate LEAs • Often regulates school technology providers (including edtech companies)
Key Provisions:	• Requires companies to obtain verifiable parental consent before collecting or disclosing data *from* children under 13 (not data *about* children under 13). ○ Schools can consent instead if the services are solely for the use and benefit of the school, and for no other commercial purpose.
Frequent LEA Concerns:	• Uncertainty about when consent is needed to use technologies. • Misconception that technology companies can pass COPPA's verifiable parental consent requirements onto schools.

Mitigating AI Risks Toolbox

Algorithmic Harms in Education

- **AI systems can inadvertently perpetuate historical biases and inequalities in the education system**
- **Algorithms are opaque and it is harder to identify when students may be harmed**
- **Students have limited control in the educational environment**
    - “Participation in…education in the United States now implicitly requires that students consent to sharing their personal information with third parties with little transparency or control over their own information.” – *Cecilia Parks*

EPIC Recommendation: Stronger Contract Language

- Improving Data Oversight and Control
- Imposing Transparency or Reporting Requirements
- Incorporating Sunsetting Clauses or Procedures to Transition Ownership to Agencies
- Requiring Human Review

Accuracy & Error in Algorithmic Systems

Some technologies used by governments are inaccurate. They don't measure or detect what they claim to, or they do it poorly. This can result in decisions that adversely affect some individuals more than others. A single error in some contexts can result in a fatal or life-altering situation.

EXAMPLE–>

Automated license plate readers *can misidentify letters and numbers on the plate or the state where the plate was issued.*

EXAMPLE–>

Facial recognition systems *are never completely accurate; photos of suspects can be incorrectly matched with mugshots in a police database and falsely identify a person.*

GOALS:

Policymakers should be able to demonstrate that:

- ❑ **The system won't make false or misleading assessments**
- ❑ **People using the system are trained to recognize situations where false results are likely**
- ❑ **Robust, auditable oversight of the system is in place.**

https://www.aclu-wa.org/AEKit/questions

Accuracy & Error in Algorithmic Systems

1. **How accurate is the system? How often and under what conditions does it make mistakes? Does it have settings to adjust for more precise predictions?**
   a. What evidence is there that the accuracy of the system has been independently tested, besides the manufacturer's claims?
   b. How will the system perform in the local context where it is being deployed? Systems should be checked for their real-world performance in the places they are used.
   c. How does the system perform when presented when presented with diverse characteristics such as skin tone, lighting, signal interference, movement, or incomplete information?
2. **What policies and procedures are in place when the system makes a mistake?**
   a. How are users of the system trained to recognize and resolve errors?
   b. How do reporting processes publicly disclose errors when they occur?
   c. What mechanisms are in place for auditing outcomes?
   d. What is the role of community oversight in monitoring errors and outcomes?
   e. What penalties exist for harms resulting from inaccurate assessments?
   f. What protections are there for whistleblowers?

https://www.aclu-wa.org/AEKit/questions

Injustice in Algorithmic Systems

Even when a system works perfectly accurately, it can still cause harm. The records that the system replies on can reflect previous discrimination, or the system can be applied in unjust ways.

EXAMPLE–> ***Applicant tracking systems*** *can replicate discriminatory hiring practices because of reliance on records of previous hiring.*

EXAMPLE–> ***A 100% accurate facial recognition system*** *could be used for harmful applications, such as identifying protestors.*

GOALS:

Policymakers should be able to explain how:

- ❑ **The system will not replicate historical patterns of bias like racism or sexism.**

https://www.aclu-wa.org/AEKit/questions

Accuracy & Error in Algorithmic Systems

1. **Where does the data that the system is using come from? Who gathered that data, with what tools, and for what purposes?**
   a. How has the data been audited to ensure it does not reflect discriminatory practices?
   b. Will the data be repurposed from the original reason it was collected? If so, how?
2. **If the system works without errors, does it still perpetuate injustice?**
   a. What say do community members have in how the system is implemented (including where and when the system is used)? Can community members object and have their objections heard?
   b. How can the public access and correct system records?
   c. What are the explicitly intended and allowable uses of the system?
   d. Are there oversight mechanisms in place to ensure that the system is only being used for the specific purposes claimed? If so, what are they?
   e. Are there any disciplinary penalties for misuse of the system? If so, what are they?

https://www.aclu-wa.org/AEKit/questions

Case Study: Getting Consent

Case Study: When Some Parents *Don't* Provide Consent

A fourth grade teacher wants to use a new edtech platform that incorporates AI functionalities with their class of 20 students. The platform would collect a variety of student PII, including student name and progress over time.

The teacher sends home permission forms with all 20 students. 16 parents sign and return the form, but 4 students in the class do not receive their parent's written consent to use the platform. **Can the teacher still use the platform in class?**

Risks Related to Education Technology

Risk	Think about…
Safety	Are students able to share personal information with others using this technology?
Permanent Record	How long does the technology retain information about your students?
Social Harm	How might educational technology contribute to or enable cyberbullying and stigmatization of your students?
Equity Concerns	What if students do not have access to information or technology?
Loss of Opportunity	Does this technology make decisions about or impact the opportunities and services your students have access to?

Risks of Sharing Data Without Adequate Privacy & Security Protections

Social Harm	Sharing personal student data may result in stigmatization and can lead to bullying.
Safety	Sharing sensitive data that has not been properly de-identified can endanger students by enabling bad actors to learn private information about them and potentially even locate them.
Loss of Control	If data is shared with too many third parties, it may be unworkable to keep track of every data flow and the school may ultimately lose control over who gets downstream data access.
Secondary Use	Without contractual limitations in place, third parties with whom data is shared may use project data for their own purposes in a way that exceeds the scope of participant consent and violates applicable laws (such as FERPA).
Autonomy	Participants have chosen to share their data with the school, not with unnamed third parties. Sharing project data with third parties without prior disclosure to participants would violate their decisional autonomy–and their trust–over who has access to their personal data.
Increased Attainability	Data that is shared without adequate security protections (such as encryption) may be intercepted by bad actors and made available to unintended third parties.

When can information covered by FERPA be shared with third parties?

1. With consent; or
2. When an exception applies.

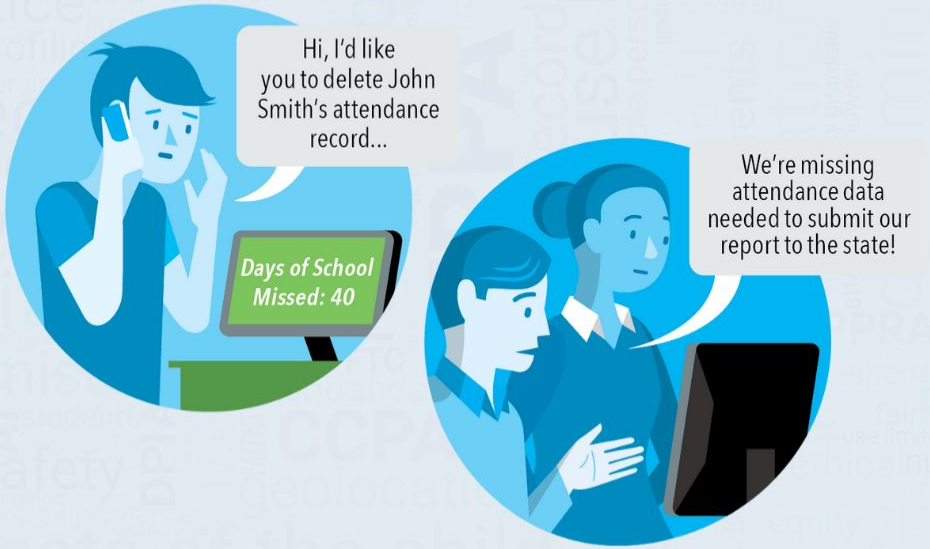
Consent

- When parents and eligible students* give **written consent**, schools can share student data with edtech companies.
- **This can't be a blanket consent** - schools can't ask parents to consent to the use of all apps you might use in the classroom that year.
- Schools also **can't pressure or force parents to consent**.

** Students under 18 cannot consent to data sharing.*

THE SCHOOL CONTEXT IS DIFFERENT

WHO CONTROLS STUDENT DATA?



STUDENT MEDICAL INFO

MATH GAMES

STUDENT GRADES

FREE LUNCH DATA, AND ALLERGIES

SCHOOL PHOTOS

ROUTE

Examples of When Parental Consent May Not Be Feasible When Sharing Student Data:

Scenario	Explanation
Student Grades	When a student transfers to a new school, their grades must go with them.
Student Medical Information	Requiring parental consent for sharing student medical information may result in students not receiving necessary care in medical emergencies.
Foreign Language App	Requiring parental consent to use a translation app with students may result in teachers not being able to communicate with english language learners.
Approved Apps	Parental consent may not be necessary if a teacher finds educational technology that has been thoroughly vetted for privacy, security, and legal compliance.
Transportation Services	Requiring parental consent to share student addresses with transportation services may result in some students not having access to reliable transportation to and from school.
Free Lunch Data	Information about student eligibility to participate in the National School Lunch Program may need to be shared with school and district staff to facilitate the program. Requiring parental consent to share this information may result in eligible students not receiving this service and going hungry.

But we also have recent laws and practices where parents have not been informed or allowed to give or refuse consent

EDUCATION WEEK

Welcome, AVance
MY ACCOUNT | LOGOUT

Browse archived issues | Current Issue | TOPICS | BLOGS | REPORTS & DATA

To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts

LEARNING & TECH

Coming To Texas: Special-Ed Cams To Protect Students From Their Own Teachers

December 15, 20

Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals.

The kids and their parents don't know.

Targeted | A Times investigation

74

DONATE

Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave

ICHAEL | ARCHIVES | SUBSCRIBE | MORE

Florida law requiring schools inquire about student mental health raises privacy concerns

Key Components of Parental Consent

- ☑️ Educational benefit of Open Generative AI tool
- ☑️ Clear explanation of what data may be collected
- ☑️ If and how data may be shared beyond students' educational purpose
- ☑️ School district liability waiver

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Common K-12 FERPA Exceptions

1. Other schools to which a student is transferring;
2. Specified officials for audit or evaluation purposes;
3. Appropriate parties in connection with financial aid to a student;
4. Organizations conducting certain studies for or on behalf of the school;
5. Accrediting organizations;
6. To comply with a judicial order or lawfully issued subpoena;
7. State and local authorities, within a juvenile justice system, pursuant to specific State law.
8. Appropriate officials in cases of health and safety emergencies;
9. School officials with legitimate educational interest;
10. Directory Information;

By Jim Siegl

The School Official Exception

*A contractor, consultant, volunteer, or other party **to whom an agency or institution has outsourced institutional services or functions** may be considered a school official under this paragraph provided that the outside party -*

(1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
*(2) Is under the **direct control** of the agency or institution with respect to the use and maintenance of education records; and*
(3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

*An educational agency or institution must use **reasonable methods** to ensure that school officials obtain access to only those education records in which they have **legitimate educational interests** [specified in the school/LEA's annual notification of rights under FERPA].*

Legalese	What It Means
Performs an institutional service or function for which the agency or institution would otherwise use its employees;	**In an ideal world, the school would do it themselves**
Is under the direct control of the agency or institution with respect to the use and maintenance of education records;	**Can the school delete on demand? Place limitations on how the vendor is using the data? How much autonomy does the vendor have to do whatever they want with the data?**
PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;	**Vendors can only use PII for the reasons why they received the PII, unless they receive additional authorization/consent from the school or parent**
Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.	**The school's notice about the school official exception has to be broad enough to encompass what the vendor is doing for them (this is almost never an issue!)**

AI Agreement Review Checklist

Data Privacy Review:

- ☑️ Open or Closed AI?
- ☑️ Is there a privacy setting?
- ☑️ Is there a data privacy agreement that meets state and national education standards?
- ☑️ Is parental consent required for student use?

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

AI Agreement Review Checklist

- ☑ Does AI platform have age requirement?
- ☑ To what extent does the platform share data input or generated by students?
- ☑ Is knowledge base limited or open for student engagement?
- ☑ Does district receive affirmative notice of software updates if AI is opened or added?
- ☑ Does the platform meet cybersecurity standards and indemnify the District in the event of a data breach?

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Case Study: When Some Parents *Don't* Provide Consent

A fourth grade teacher wants to use a new edtech platform that incorporates AI functionalities with their class of 20 students. The platform would collect a variety of student PII, including student name and progress over time.

The teacher sends home permission forms with all 20 students. 16 parents sign and return the form, but 4 students in the class do not receive their parent's written consent to use the platform. **Can the teacher still use the platform in class?**

Case Study: Student Data Used to Train AI

Case Study: Using Student Data to Train Algorithms

An edtech company that provides a math app for use in K-12 schools receives student PII under FERPA's school official exception.

The company would like to use student PII collected on the platform to train a new algorithm that will personalize learning in the science app they are developing. **Is this permissible?**

The School Official Exception

*A contractor, consultant, volunteer, or other party **to whom an agency or institution has outsourced institutional services or functions** may be considered a school official under this paragraph provided that the outside party -*

(1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
*(2) Is under the **direct control** of the agency or institution with respect to the use and maintenance of education records; and*
(3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

*An educational agency or institution must use **reasonable methods** to ensure that school officials obtain access to only those education records in which they have **legitimate educational interests** [specified in the school/LEA's annual notification of rights under FERPA].*

Legalese	What It Means
Performs an institutional service or function for which the agency or institution would otherwise use its employees;	**In an ideal world, the school would do it themselves**
Is under the direct control of the agency or institution with respect to the use and maintenance of education records;	**Can the school delete on demand? Place limitations on how the vendor is using the data? How much autonomy does the vendor have to do whatever they want with the data?**
PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;	**Vendors can only use PII for the reasons why they received the PII, unless they receive additional authorization/consent from the school or parent**
Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.	**The school's notice about the school official exception has to be broad enough to encompass what the vendor is doing for them (this is almost never an issue!)**

Parent / Guardian Consent May Be Required Because Open Generative AI Likely Exceeds FERPA Exception

- **Collecting student data which populates AI knowledge base beyond school setting likely goes beyond a “legitimate educational interest.”**
- **Populating AI knowledge base with student inserted content is also likely resharing student data beyond the scope of the original purpose of the educational software.**

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Under COPPA, a school can consent on a parent's behalf only when:

- The data collected is used only for a school authorized educational purpose;
- The company provides the school notices required under COPPA;
- If the school requests it, the company provides the school a description of the types of personal information collected; an opportunity to review a child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information; and
- Operators to delete children's personal information once the information is no longer needed for its educational purpose.
- The FTC also recommends that, as a best practice, schools consider sharing the notices provided by the company with parents and allowing parents the ability to review personal information collected.

Case Study: Using Student Data to Train Algorithms

An edtech company that provides a math app for use in K-12 schools receives student PII under FERPA's school official exception.

The company would like to use student PII collected on the platform to train a new algorithm that will personalize learning in the science app they are developing. **Is this permissible?**

Case Study: Self-Harm and Threat Monitoring

Case Study: Self-Harm Monitoring

A school contracts with a technology company to track and record all student activity on school-issued devices, school-owned accounts, and the school's Wi-Fi network, notifying the school if the algorithm flags that an intervention could be necessary. The software flags that a student is highly likely to imminently harm themselves. **Can the school–or the technology company–notify law enforcement based solely on the algorithm's flag?**

Monitoring Students

School-issued devices like laptops typically contain location-tracking technology. Schools may monitor activity on password-protected sites, including email and social media.

Children's Internet Protection Act (CIPA)	
High-Level Overview:	• Requires entities receiving E-Rate funding to filter and monitor internet content on their networks.
Applicability to LEAs:	• Directly regulates LEAs receiving E-Rate funding
Key Provisions:	• Schools and libraries subject to CIPA are required to create an internet safety policy that includes technological protection measures that block or filter access to obscene online content. CIPA also requires schools to monitor students' online activities, and how they do so must be referenced in schools' internet safety policies.
Frequent LEA Concerns:	• Uncertainty about how much filtering and monitoring is sufficient to comply with the law but not infringe on student and parent privacy and other rights.

Student Monitoring

School-Issued Devices

Any device that the school issues to a student, such as laptops or tablets, may be monitored. The monitoring system may access and process any online data from these devices, potentially including students' online activities when they use these devices at home.

School-Managed Internet Connections

Any online data from any school-managed internet connection may be monitored, including students' online activities using a take-home Wi-Fi internet hotspot. Students who use personal devices may nonetheless have their online activities subject to monitoring if they connect to a school-managed network, whether at school or at home.

School-Managed Apps and Accounts

Certain student accounts that are managed by the school may be monitored (e.g. Microsoft 365 or Google Workspace), regardless of the internet connection or device that a student uses to access the accounts. For example, depending on the school-managed account and the capabilities of the monitoring system, students who access their school-managed email accounts, videoconferencing or chat applications, or document storage accounts, from a personal device using a non-school

internet connection at home may have their activities monitored. This is because the monitoring occurs at the level of the school-managed app, not at the level of the device or internet connection.

Without the assurance of privacy protections, students are both less likely to seek out help when they need it and less likely to engage openly with mental health counselors or other service providers.

- Bazelon Center testimony before the Federal School Safety Commission

AI Agreement Review Checklist

Threat Monitoring:

- ☑ Is student chatbot or AI prompt engagement monitored?
- ☑ Is there a threat assessment feature?
- ☑ Is there a “human in the loop”?
- ☑ Does the district have resources and protocol to adequately respond?
- ☑ Is there an indemnification provision for monitoring and alerts by software company?

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Case Study: Self-Harm Monitoring

A school contracts with a technology company to track and record all student activity on school-issued devices, school-owned accounts, and the school's Wi-Fi network, notifying the school if the algorithm flags that an intervention could be necessary. The software flags that a student is highly likely to imminently harm themselves. **Can the school–or the technology company–notify law enforcement based solely on the algorithm's flag?**

The Health and Safety Exception

- **Standard:** actual, impending, or imminent emergency and a school must determine whether an “articulable and significant threat” exists on a case-by-case basis, taking into account the totality of the circumstances pertaining to a threat to the health or safety of a student or others (USEd, FERPA FAQs)

Case Study: Self-Harm Monitoring

A school contracts with a technology company to track and record all student activity on school-issued devices, school-owned accounts, and the school's Wi-Fi network, notifying the school if the algorithm flags that an intervention could be necessary. The software flags that a student is highly likely to imminently harm themselves. **Can the school–or the technology company–notify law enforcement based solely on the algorithm's flag?**

But most of the time, it is a harder call. So: How could risks be reduced or eliminated?

Risk	Options to reduce or eliminate risk	Effect on risk

Case Study: Generating IEPs

Case Study: Using Generative AI to Help Write IEPs

A teacher uses ChatGPT to help them draft IEPs for students with disabilities. The teacher is careful not to enter student names or student ID numbers, but does include details about each student's disability and their learning progress. **Is this permissible?**

FERPA and AI

- **AI can increase the risk of re-identification**
  - FERPA has a fairly high standard for de-identification: whether "a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances [could] identify the student with reasonable certainty" (34 CFR § 99.3)
    - Proper de-identification "involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or masked." (PTAC, Frequently Asked Questions—Disclosure Avoidance)
  - Directory information: "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." (34 CFR § 99.3)
  - "the risk of re-identification may be greater for student data than other information" because of the large amount of student data that is disclosed, including de-identified data and directory information. (73 Fed. Reg. 74,834)

De-identification and FERPA

A few reminders:

- **FERPA's definition of PII includes anything linked or linkable to the student - a higher standard than HIPAA!!!**
- **Aggregate data may still contain PII**
- **Removing direct identifiers is rarely sufficient to de-identify individual-level data.**
- **FERPA does not have a "Safe Harbor" de-identification standard.**
- **There may be unpleasant consequences for not safeguarding student data: The Five Year Ban!**

Additional Examples of AI in Education

Biometrics for Quick ID Purposes

Some schools use eye scanners and palm prints instead of student ID cards. **What legal and ethical guardrails need to be in place?**

Biometrics for Other Purposes

Students may be asked to wear heart-rate monitors in PE, and grades may be based on how hard a student works out.

Students may wear devices that record their activity during the day and night. The data can be used for reports available to parents and administrators.

What legal and ethical guardrails need to be in place?

Student Success Trackers & Early Warning Systems

Companies collect student data–such as demographic information, free or reduced lunch status, whether they've used drugs, etc.–and then use that data for predictive analytics to analyze for warning signs related to not being on track to graduate on time so that they can do interventions.

What legal and ethical guardrails need to be in place?

Parent / Guardian Consent May Be Required Because Open Generative AI Likely Exceeds FERPA Exception

- **Collecting student data which populates AI knowledge base beyond school setting likely goes beyond a “legitimate educational interest.”**
- **Populating AI knowledge base with student inserted content is also likely resharing student data beyond the scope of the original purpose of the educational software.**

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law

Key Components of Parental Consent

- ☑️ Educational benefit of Open Generative AI tool
- ☑️ Clear explanation of what data may be collected
- ☑️ If and how data may be shared beyond students' educational purpose
- ☑️ School district liability waiver

https://youtu.be/Fvzm2o7hou0?si=mqXFweD5sl6EnqDt

F3 Law