

Safeguarding Student Data: Navigating Legal, Ethical, and Privacy Implications

SETA-ED

**We WANT
your input!**



SESSION PRESENTERS



Dr. Imani Goffney

Ast. Prof, Univ of
Maryland



Dr. Melina Uncapher

CEO, SETA-ED



Amelia Vance

President, Public
Interest Privacy
Center

Adj. Prof, William &
Mary Law

Agenda

- Competing Tensions
- Defining Privacy
- How to Prioritize: Risk Analysis
- Risk Matrix

**We WANT
your input!**





Competing Tensions

To appropriately **balance** the potential **benefits** of educational technology and data use by managing the **privacy, security and safety risks**.

Providing students with
technology-enhanced
opportunities

Privacy and confidentiality

Transparency
and trust building

Speed and availability
of innovation



Carefully vetting
technologies

Pressure to quickly adopt
new technologies

Recognizing equity and
justice issues

Efficiency and functionality

What are the competing tensions you face?



Defining Privacy



Defining Privacy

The responsible, ethical, and equitable collection, use, sharing, and protection of child and student data.

Respecting Privacy

The success of your programs and teams are governed by:

- Local, state, and federal privacy laws and regulations
- Technical safeguards
- Ethical norms
- Social license: legitimacy, credibility, and public trust.

When privacy isn't adequately supported

- Failing to address stakeholders' privacy perceptions and concerns—even with strong privacy safeguards in place—can disrupt or conclude your research

Why Children Need Additional Protections*

- Brains are not fully developed
- Lack of experience
- Different conception of privacy
- Potentially more acute harms

*But they also need protections the day they turn 18!!!



Privacy Benefits

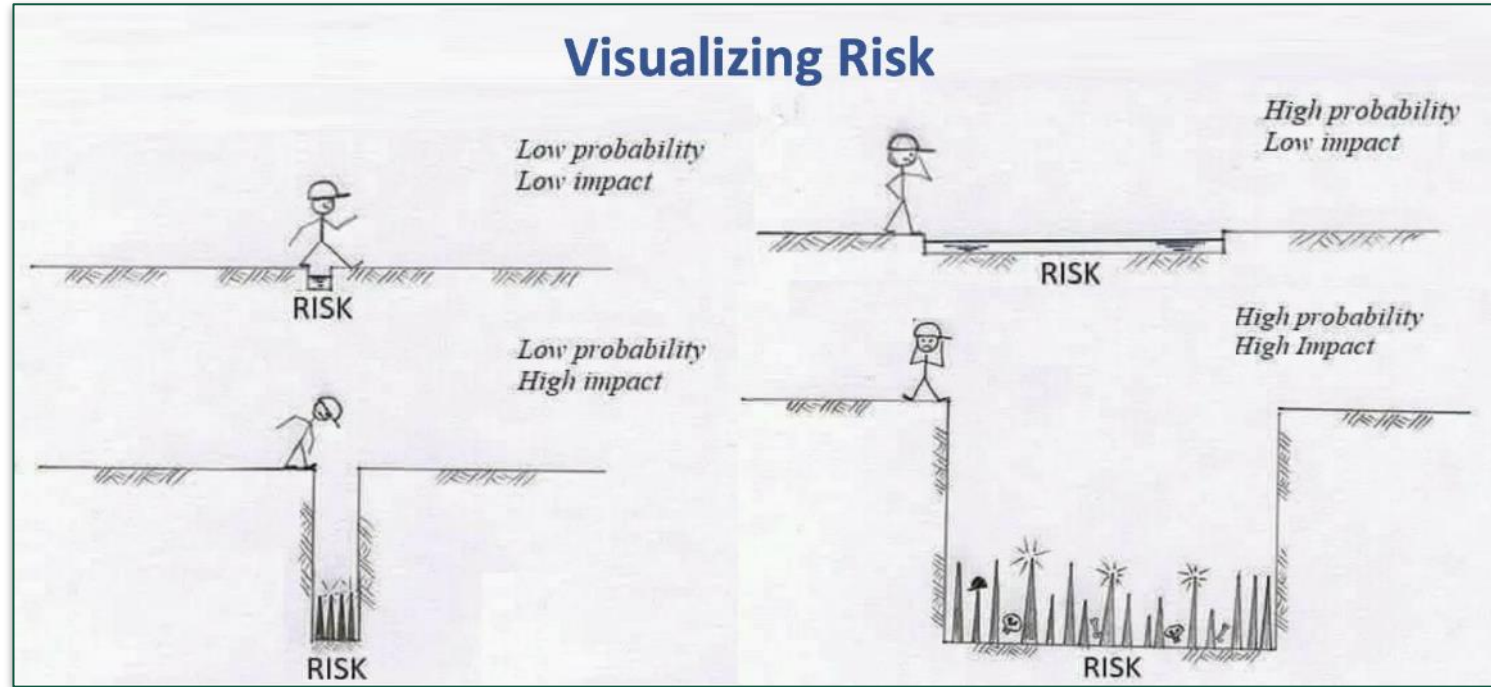
Identity allows us to be thinking, self-defining humans; freedom lets us be citizens; and protection safeguards our roles as situated consumers and workers, allowing us, as members of society, to trust and rely on other people so that we can live our lives and hopefully build a better future together.

Neil Richards



How to Prioritize: Risk Analysis

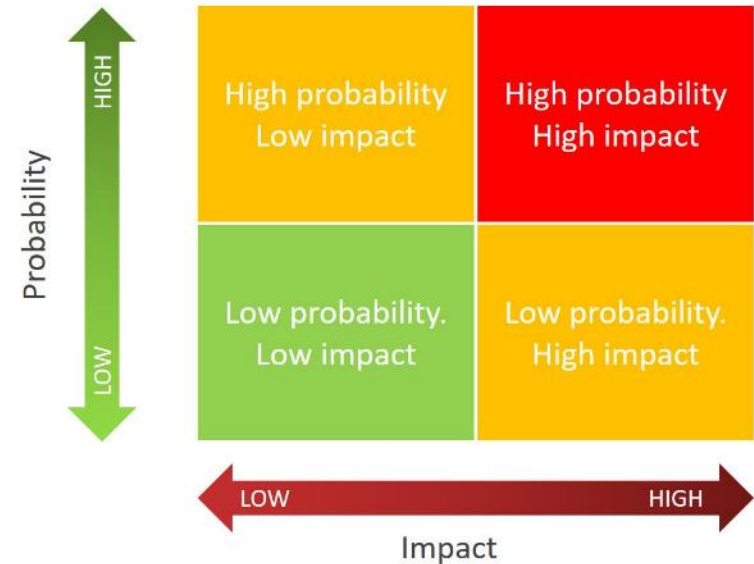
Risk Analysis



Privacy Risks Are Often Not Immediately Apparent

Privacy risks can be...

- Incremental
- Unequal
- Not obvious
- Intrusive



Risks of Sharing Data Without Adequate Privacy & Security Protections

Social Harm	Sharing personal student data, especially data related to priority population status, 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 for AERDF to keep track of every data flow and AERDF 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 AERDF, not with unnamed third parties. Sharing project data with third parties without prior disclosure to participants would violate their decisional autonomy 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.

Risks of Sharing and Repurposing Data Across Systems

- Misunderstanding or Misusing Student Data
 - Circumventing Privacy Laws, Including FERPA
 - Undermining Students' and Families' Expectations of Privacy
 - Discouraging Students from Providing Information or Seeking Help
- Increased Risk of Security Breaches and Human Error
- Perpetuating Bias, Creating Permanent Records, and Long-Term Negative Effects
- Take Care When Sharing Data with Law Enforcement

What Does Harm Look Like in Education?

- According to a complaint filed with the FTC, ~60,000 eighth-grade students have been assigned to play a math game by their teacher. While the game is free when students play in a restricted mode with only their classmates, children playing the unrestricted version of the game received regular reminders and messages encouraging them to become members, which costs \$59.88 to \$107.40 per child per year. - [NBC News](#)
- Chicago Public Schools disclosed school public spending as part of its commitment to transparency. Information was not redacted on spending for special education student services. This information was in spreadsheets downloadable for anyone who accessed their website, with data available between 2013 and 2016. In just the 2015-2016 records, there were 1,600 instances where student names and their services were listed. - [Chicago Sun-Times](#)

What Does Harm Look Like in Education?

- Des Moines Public Schools accidentally published seven documents publicly that included names and descriptions of students requesting transfers to different school districts. The documents included why students were transferring, identifying by name students who were bullied and physically or sexually assaulted. The documents had been moved to a folder in the school district's online system that was not flagged to remain private, causing the documents to become publicly viewable. - [We Are Iowa](#)
- Hacking group "The Dark Overlord" hacked small school districts in various states. They then used the data to text death threats to parents, sent random letters to school administrators referencing the shooting at Sandy Hook Elementary School and threatening public release of student health and discipline information, and posted a student directory online so "any child predator can now easily acquire new targets and even plan based on grade level." Many of the targeted school districts had to shut down for multiple days as the threats were investigated - [The Daily Beast](#); [The Washington Post](#); [Cyberscoop](#).

What Does Harm Look Like in Education? (cont'd)

- Oklahoma University unintentionally exposed thousands of students' educational records—including social security numbers, financial aid information and grades in records dating to at least 2002--through lax privacy settings in a campus file-sharing network, violating federal law. - [OU Daily](#)
- In March 2021, Dartmouth charged 17 medical student with cheating based on a review of certain online activity data on Canvas (the learning management system) during remote exams—despite Canvas stating multiple times that the activity data shouldn't be used for this purpose. The school dropped 7 of the cases after students argued that administrators had mistaken automated Canvas activity for human cheating. The 10 others were expelled, suspended, or received course failures and unprofessional-conduct marks on their records. These punishments were later reversed after extensive media coverage - [The New York Times](#)

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.

The Challenge: Allow Opportunities for Youth Online While Mitigating Risks

Physical Harm

Does the research involve any risks to participants?

Is there a risk of physical harm to participants, such as through participation in dangerous activities or adverse effects from interventions or exposure to research materials?

Psychological/ Emotional/ Mental Harm

Does the research involve any psychological or emotional risks to participants, such as stress or discomfort? Is there a risk of harm to participants, such as through exposure to sensitive content or experiences?

Risk Matrix

Table 1: Risk Determination Checklist for Traditional Research

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
Physical Harm	Does the research involve any physical risks to participants? Is there a risk of physical harm to participants, such as through participation in dangerous activities or adverse side effects from interventions or exposure to research materials?			High/ Medium/ Low	Use appropriate safety measures and minimize any potential risks to participants, obtain informed consent and provide participants with clear information about potential risks, and provide access to medical support if needed. Ensure proper training for researchers.
Psychological/ Emotional/ Mental Harm	Does the research involve any psychological or emotional risks to participants, such as stress or discomfort? Is there a risk of harm to participants, such as through distressing or sensitive content or experiences?			High/ Medium/ Low	Provide participants with clear information about the nature of the research and any potential risks, offer support services to participants if needed. Obtain informed consent from participants, ensure anonymity and confidentiality and that participants have the right to withdraw at any time.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
Confidentiality Breaches	Is there a risk that participants' personal or identifiable information could be disclosed? Is there a risk of breaching confidentiality, such as through unauthorized access to data or accidental disclosure?			High/ Medium/ Low	Use appropriate measures to protect confidentiality, such as data encryption and secure storage, limit access to data, and obtain consent for any identifiable information that will be collected from participants and inform them of the risks.
Vulnerability	Are participants in the research considered vulnerable, such as children, individuals who might be less than fluent in English, economically disadvantaged individuals, elderly, or individuals with disabilities?			High/ Medium/ Low	Use additional safeguards to protect vulnerable participants, such as involving their legal guardians or caregivers in the informed consent process, ensuring that the research is age-appropriate and respectful of their capabilities, and providing additional support services as needed. To address communication obstacles, such as language differences, use various means, including advocates, translators/interpreters, sign language experts, or technology.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
Power Imbalances	Is there a risk of power imbalances between the researcher and participants, such as through coercion or manipulation? Are there any power imbalances that could impact the research process or outcomes?			High/ Medium/ Low	Minimize power imbalances by using appropriate communication and consent procedures, and by ensuring that participants have the right to withdraw from the research at any time. Use appropriate methods to ensure participants are aware of their rights and are free to make their own decisions, and provide support services to participants.
Informed Consent	Have participants been provided with clear and understandable information about the research and given the opportunity to provide informed consent? Are participants fully informed about the nature, risks, and benefits of the research, and have they given voluntary and informed consent to participate?			High/ Medium/ Low	Use plain language and visual aids to explain the research and obtain informed consent, consider alternative forms of consent for those with limited literacy or cognitive abilities. Provide participants with clear and understandable information about the research, use appropriate methods to obtain informed consent (e.g. written consent), and ensure that participants have the right to withdraw at any time.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
Data Management	Are there any risks to the management or storage of research data, such as data loss or unauthorized access?			High/ Medium/ Low	Use appropriate data management practices, such as secure storage, data encryption and data backup. Ensure that only authorized personnel have access to the data and that any data collected is stored in accordance with applicable regulations and guidelines.
Cultural Sensitivity	Are there any cultural factors that need to be considered in the research, such as language or cultural practices?			High/ Medium/ Low	Ensure that the research is culturally sensitive and respectful. Use appropriate translation or interpretation services if needed.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
Privacy	Is there a risk of invasion of privacy, such as through unauthorized observation or recording of participants?			High/ Medium/ Low	Obtain consent for any observation or recording of participants, use appropriate methods to ensure privacy is respected, and ensure that any data collected is anonymized.
Deception	Does the research involve any deception of participants, such as withholding information or providing false information?			High/ Medium/ Low	Only use deception if it is necessary and justified by the research question. Obtain informed consent from participants and debrief them afterwards.

Table 2: Risk Determination Checklist for UX/UI or Design-Based Research

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
User Privacy	Is there a risk of invasion of user privacy, such as through unauthorized access to user accounts or data? Are there any additional considerations for respecting the privacy of research participants?			High/ Medium/ Low	Obtain consent for any access to user accounts or data, use appropriate methods to ensure user privacy is respected, and ensure that any data collected is anonymized. Consider any additional measures needed for respecting the privacy of research participants, such as providing clear privacy policies or offering alternative methods for participation.
Accuracy of Results	Is there a risk of inaccurate results, such as through biased sampling or flawed data analysis? Are there any additional considerations for ensuring the accuracy of results for UX/UI research?			High/ Medium/ Low	Use appropriate sampling methods to ensure representative samples, use appropriate statistical methods to analyze data, and consider any potential biases in the research design. Consider any additional measures needed for ensuring the accuracy of results for UX/UI research, such as using multiple data sources or user feedback to validate results.
© Access 4 Learning (A4L) Community and PESCE  					

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
User Experience	Is there a risk of negative user experience, such as through confusing or frustrating interfaces or tasks? Are there any additional considerations for ensuring positive user experience in the UX/UI research?			High/ Medium/ Low	Use appropriate methods to ensure positive user experience, such as user testing and feedback, and consider any potential barriers to user experience, such as language or accessibility issues. Consider any additional measures needed for ensuring positive user experience in UX/UI research, such as providing clear instructions or offering alternative methods for participation.
Third-party Services	Is there a risk of third-party services compromising user data or privacy, such as through unauthorized data access or sharing? Are there any additional considerations for using third-party services in UX/UI research?			High/ Medium/ Low	Use third-party services with appropriate data protection policies and agreements, limit the amount of data shared with third-party services, and obtain consent for any use of third-party services. Consider any additional measures needed for using third-party services in UX/UI research, such as auditing third-party services for data protection policies or using alternative services with better data protection policies.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
User Vulnerability	Is there a risk of vulnerable users being exploited or harmed through the research, such as through excessive demands or inappropriate content? Are there any additional considerations for ensuring the safety of vulnerable users in UX/UI research?			High/ Medium/ Low	Use appropriate methods to ensure the safety of vulnerable users, such as obtaining additional consent
User Safety	Is there a risk of harm to users, such as through physical injury, emotional distress, or exposure to inappropriate content?			High/ Medium/ Low	Use appropriate methods to ensure user safety, such as providing clear instructions, warnings, and safety guidelines. Avoid using inappropriate or offensive content, and provide adequate support services for users who may experience emotional distress.

Risk Categories	Risk Questions	Yes	No	Risk Level	Mitigation Strategies
User Bias	Is there a risk of biased or unfair treatment of users, such as through discriminatory algorithms or biased data collection methods?			High/ Medium/ Low	Use appropriate methods to ensure fair and unbiased treatment of users, such as using representative samples and appropriate statistical methods. Avoid using discriminatory algorithms or biased data collection methods, and provide transparency and accountability in the decision-making process.
Covert Research	Does the study use any covert research methods?			High/ Medium/Low	Avoid covert research methods whenever possible, as data can generally be collected via less intrusive methods. If covert research is unavoidable, fully disclose the covert data collection and how it works as part of the informed consent process. After data have been analyzed, delete raw data as quickly as possible.

Table 3: Community and Reputational Risks

<i>Risk Level</i>	<i>Description</i>	<i>Yes</i>	<i>No</i>	<i>Potential Consequences</i>	<i>Mitigation Strategies</i>
High	Research involves collecting personal or sensitive data that could lead to potential privacy violations			Legal action, loss of trust, reputational damage	Obtain informed consent, ensure data protection and confidentiality, minimize data collection.
High	Research involves people from vulnerable populations or different cultural backgrounds			Harm, legal action, offense, loss of trust	Conduct cultural sensitivity training, involve diverse user groups, obtain informed consent and/or assent, use opt-in consent whenever possible.
High	Research involves physical or psychological risks to the users			Harm, legal action, loss of trust	Obtain informed consent, ensure user safety and well-being, use appropriate methods and equipment, use opt-in consent whenever possible.

<i>Risk Level</i>	<i>Description</i>	<i>Yes</i>	<i>No</i>	<i>Potential Consequences</i>	<i>Mitigation Strategies</i>
Medium	Research touches on politically sensitive issues or topics			Backlash, negative consequences, reputational damage	Consult legal and public relations teams, obtain informed consent, limit access to sensitive data
Medium	Research may cause negative reactions or opinions from stakeholders			Loss of trust, reputational damage, legal action	Involve stakeholders in the research process, communicate findings transparently, address concerns and feedback
Low	Research does not involve any significant risks to users or stakeholders			Minimal consequences	Follow ethical guidelines and best practices, obtain informed consent, communicate findings transparently

Table 4: Risk Assessment Matrix

<i>Likelihood / Impact</i>	<i>Low likelihood</i>	<i>Moderate likelihood</i>	<i>High likelihood</i>
<i>Low severity</i>	- No significant risk (R&D), low ethical risk (HSR) - Minor ethical concerns. - May not require additional review. - Standard review (RDEC)	- Low to moderate risk, (R&D), moderate ethical risk (HSR) - Moderate ethical concerns. - May require additional review and mitigation measures - Full committee review (RDEC)	- Moderate to high risk (R&D), high ethical risk (HSR) - Significant ethical concerns - Requires additional review and significant mitigation measures. - Full committee review (RDEC) and external IRB required
<i>Moderate severity</i>	- Low to moderate risk (R&D), moderate ethical risk (HSR) - Moderate ethical concerns - May require additional review and mitigation measures - Full committee review (RDEC)	- Moderate ethical risk (R&D), high ethical risk (HSR) - Some significant ethical concerns - Requires additional review and mitigation measures. - Full committee review (RDEC) and external IRB	- High ethical risk (R&D), very high ethical risk (HSR) - Significant ethical concerns - Requires additional review and significant mitigation measures - Full committee review (RDEC) and external IRB

<i>Likelihood / Impact</i>	<i>Low likelihood</i>	<i>Moderate likelihood</i>	<i>High likelihood</i>
<i>High severity</i>	- Moderate ethical risk (R&D), high ethical risk (HSR) - Significant ethical concerns - Requires additional review and mitigation measures. - Full committee review (RDEC) and external IRB	- High ethical risk (R&D), very high ethical risk (HSR) - Significant ethical concerns - Requires additional review and significant mitigation measures - Full committee review (RDEC) and external IRB	- Very high ethical risk (R&D), critical ethical risk (HSR) - Significant ethical concerns - Requires additional review and significant mitigation measures, and may not be ethically justifiable - Full committee review (RDEC) and external IRB

Questions?

Thank you for coming!

Contact information:

Dr. Melina Uncapher: melina@seta-ed.com

Amelia Vance: avance@publicinterestprivacy.com

Dr. Imani Masters Goffney: igoffney@umd.edu