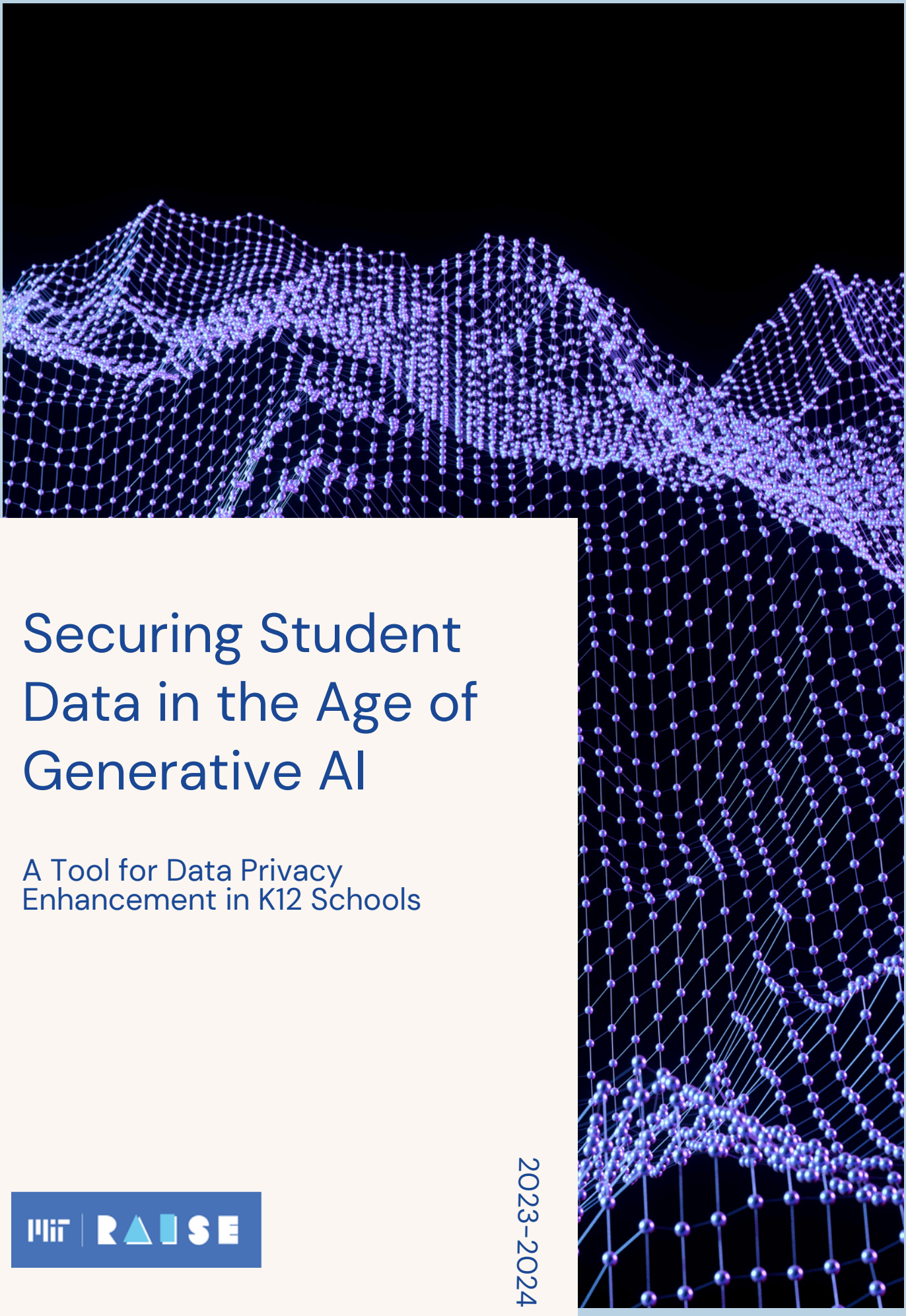


Securing Student Data in the Age of Generative AI

A Tool for Data Privacy Enhancement in K12 Schools

MIT | RAISE

2023-2024

A project for the **Massachusetts Institute of Technology Responsible AI for Social Empowerment and Education**.

by

Anjali A. Nambiar
MPA Candidate
University of California, Berkeley
Spring 2024

mail to: anjalinambiar@berkeley.edu

Table of Contents

Executive Summary

The integration of educational technology in schools has become increasingly prevalent in recent years. According to the Edtech Top 40 report by Instructure over 2500 Education Technology applications were used in schools across the country. Alongside this trend, the use of Artificial Intelligence (AI) tools in classrooms has experienced a rapid surge. Reach Capital identified at least 280 EdTech tools incorporating Generative AI into their applications. These AI EdTech platforms rely heavily on the data they collect from users, including students and teachers, to provide personalized learning experiences and insights. The data could include sensitive information about students such as academic performance, behavior patterns, and personal preferences. This accumulation of data could expose students to potential risks, including unauthorized access, data breaches, and misuse of personal information. Currently, we have seen over 1600 data breaches in school districts across the country and it will only increase with AI UK's National Cyber Security Centre warns that "Artificial intelligence (AI) will almost certainly increase the volume and heighten the impact of cyber attacks over the next two years".

There are clear advantages to using AI tools in the classroom, but it is also evident that there might be increased data risks if we are not careful. Some of the possible issues that could be aggravated by Gen AI EdTech tools are:

- Higher rates of Data breaches in schools
- Newer and advanced cyber security threats
- Safety measures may be compromised due to the strong incentive for heightened data collection, storage, and usage by AI platforms

Through a thorough analysis of literature, current available mechanisms for harm reduction, semi-structured interviews with experts and concerned stakeholders, this report offers a strategic tool that supports school-level stakeholders, namely, teachers, parents, and school administrators in reducing their risk of data privacy threats. It will aid these stakeholders by equipping them with a framework that leads to immediate reduction of data risks of the AI EdTech tools, increased awareness and security at minimum cost. It is intended to be highly practical in applicability and stay relevant for the long term in times of rapid tech changes.

The tool is designed around 4 key domains or focus areas to ensure complete protection of students, namely

- **Transparency of Data collection and Usage**
- **Privacy Regulation Compliance**
- **Redressal Mechanisms**
- **Update and Review Mechanisms**

It proposes guidelines for all identified key stakeholders and provides an interactive framework for evaluating both the security level of an EdTech platform and the security measures within schools.

Since processes and the people behind them are critical in ensuring the efficacy of the framework, the report also offers a detailed RACI structure for the implementation of these guidelines inside the school, with support from the EdTech vendors. The tool is seen as the first step in the awareness-building process to address concerns regarding data at the school level and will continue to be developed further and complemented with training and other resources that the RAISE lab will provide in the future.

This project is a part of the MIT Responsible AI for Social Empowerment and Education (RAISE) initiative, which builds upon the group's previous AI EdTech policy recommendations and roadmap for the use of Gen AI in the classroom.

The white paper by MIT on the roadmap for the use of Gen AI in K-12 education highlights the challenge posed by data collection through AI tools, emphasizing the importance of awareness among all stakeholders regarding the data collection practices of "free" generative AI platforms. It underscores the need to ensure that sensitive information is not inadvertently shared and encourages educators to stay informed about how to evaluate these tools effectively.

It is also particularly timely given the current federal initiatives aimed at regulating AI usage within educational settings. This urgency is underscored by reports such as "Artificial Intelligence and the Future of Teaching and Learning" released by the U.S. Department of Education's Office of Educational Technology.

The report advocates for clear limitations on the collection, usage, transfer, and maintenance of personal data, including restrictions on targeted advertising. It emphasizes the importance of shifting the burden onto platforms to minimize data collection rather than placing it on individuals to navigate complex legal documents.

Generative AI and data privacy in the classroom

There has been a remarkable surge in the integration of Generative AI into EdTech tools over the past few years. These tools offer innovative approaches to engage students, support educators, and enhance educational ecosystems within schools. When utilized thoughtfully and appropriately, they have the potential to revolutionize the learning process, equipping students for a digital future driven by Generative AI.

As outlined in the GenAI K12 white paper from MIT RAISE, Generative AI presents an opportunity to reimagine education to better serve the needs of students in today's context. However, it also presents a "jagged frontier," with uncertainties regarding long-term adoption and implications in education, yet promising significant advancements in classroom practices.

The sudden emergence and adoption of this technology, particularly its broader accessibility among populations less versed in technology, has caused a stir, eliciting varied reactions from school administrators. Some have sought guidance from higher authorities to establish a stance, while others have taken proactive steps, such as drafting AI adoption guidelines for their districts (as seen in the Florida ChatGPT AI policy article).

Parents and caregivers, though secondary consumers in this context, have voiced concerns and, in some instances, taken localized action.

Incidents like the cyberattack on Illuminate Education, a leading provider of student-tracking software, exposing the personal information of over a million current and former students, including names, dates of birth, races or ethnicities, test scores, and, in some cases, more intimate details like tardiness rates, migrant status, behavior incidents, and descriptions of disabilities, underscore the necessity for stronger data governance by EdTech companies.

Given the vast amounts of student data being captured, the educational market ranks as the third-highest target for data hackers, trailing only the health and financial sectors. Since 2016, the K-12 Cyber Incident Map has documented a total of 1619 publicly disclosed school cyber incidents affecting U.S. school districts.

With the introduction of Generative AI in EdTech, a myriad of data privacy and security challenges are emerging, which will be discussed in detail later in this paper.

Educational market ranks the **third-highest target for data hackers**, trailing only the health and financial sectors.

1,619

cases of cyber attacks in schools since 2016*

*as per The K-12 Cyber Incident Map by K12 SIX

Additional privacy concerns due to Gen AI integration

In addition to all the data privacy-related issues associated with the usage of traditional technology platforms in the classroom, Gen AI poses a greater vulnerability. This is because it involves many dynamics associated with data, from using it to train the model to thriving on user input and customizing the output based on the data that users input. These complex interactions between such models and data make data privacy even more challenging to ensure in the case of AI applications.

As per the study " Unveiling security, privacy, and ethical concerns of ChatGPT" specific challenges solely associated with Gen AI are as follows:

Privacy leakage due to personal input exploitation: Imagine an AI EdTech tool collects students' browsing history to personalize learning. If this data is shared with advertisers without consent, it breaches privacy. Even if it's stored insecurely and accessed by unauthorized parties, it poses risks.

To prevent such breaches, strict data protection measures and transparent data practices are essential.

Emerging new privacy attacks on LLMs such as "Jailbreaking": In the context of Large Language Models (LLMs) like ChatGPT, users could potentially reverse engineer or "Jailbreak" the system to access information from previous conversations stored in its memory. For instance, if someone manages to exploit a vulnerability in the LLM's security, they could extract sensitive data from student users' interactions, compromising privacy. This highlights the importance of robust security measures and encryption protocols to safeguard users' information in AI chat interfaces.

A solution that helps ensure student data is not shared with third parties and helps students and other stakeholders be cautious of the data they enter into the application while interacting with it would be required to safeguard students' privacy against challenges unique to GenAI tools.

Current Mechanisms for Harm Reduction

Within the education ecosystem, numerous stakeholders grapple with the significant influence of AI on children's learning experiences. Amidst this dynamic landscape, diverse actors are striving to navigate and understand the implications of AI integration. Researchers and think tanks have produced extensive documentation outlining the potential benefits of AI in education, often overlooking crucial aspects of data privacy. Established entities like Common Sense Media have developed comprehensive metrics for evaluating AI tools in classrooms, underscoring the growing importance of data security. Concurrently, parents and private entities are actively developing tools to assess the data security of AI technologies. However, these tools vary widely in complexity, ranging from dense and technical to broadly focused, with some prioritizing integration over data privacy considerations. Here is an overview of the existing landscape of policies or initiatives to ensure better student data protection:

Policies by Federal Agencies for Student Data Protection:

- Family Education Rights and Privacy Act (FERPA):Enacted in 1974 and overseen by the Department of Education, FERPA regulates the release of student information by schools. It mandates parental oversight and transparency regarding the use of student data but does not require schools to establish specific security controls.
- Child Online Privacy Protection Act (COPPA):Congress enacted COPPA to regulate business practices for collecting data from children online. Administered by the Federal Trade Commission, COPPA governs the collection and use of children's personally identifiable information (PII) by online operators.
- Kids Online Safety Act (KOSA):Undergoing scrutiny in the Senate, KOSA mandates measures to protect minors from online risks. It applies to platforms accessed by minors, requiring reasonable measures to prevent and address harms like sexual exploitation and cyberbullying. Covered platforms must offer privacy settings for minors and provide parental oversight tools.
- K-12 Cybersecurity Act:The first federal law specifically addressing K-12 cybersecurity, this legislation requires the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a study on cybersecurity risks facing the K-12 sector and provide recommendations for enhancing school defenses.
- AI in Teaching and Learning Guidelines: Issued by the Department of Education's EdTech team, these guidelines outline principles for adopting technology in the classroom. However, they also raise concerns about data usage and security aspects of AI tools, with no clear mechanisms for addressing potential privacy limitations.

Students Privacy Policy Office at the Department of Education : Provides guidelines to the education community on data privacy and governance mechanisms through resources such as checklists, guiding documents and training.

Limitations:
While these policies endeavor to protect student data, their origins in the 1970s render them outdated in the face of modern technological advancements, particularly concerning emerging technologies like AI. They lack the necessary clarity and specificity to provide schools with actionable directives on accountability and effective risk reduction strategies. The absence of clear mechanisms to address data usage and security aspects of AI tools highlights the urgent need for updated and comprehensive privacy frameworks tailored to the evolving educational landscape.

Third-Party Security Certification for EdTech Vendors:

Third-party security certification organizations, such as iKeepSafe , Education Framework or 1EdTech, offer data security services to EdTech vendors. These vendors can enlist these organizations to evaluate their platforms, leading to certifications of compliance with data safety regulations like FERPA and COPPA. Despite the potential benefits of third-party security certifications, there are significant privacy limitations to consider:

Limitations:

- Efficacy of Data Breach Reduction: While these certification processes may enhance credibility by indicating improved data practices, there is a lack of evidence demonstrating their effectiveness in reducing data breaches.
- Accountability in Breach Scenarios: The certification process does not necessarily hold organizations accountable in the event of a data breach, raising questions about the efficacy of these measures in ensuring robust data protection and accountability.

Private Initiatives for Privacy Evaluation:

Several private organizations, spurred by concerned parents or citizens, have developed various tools to raise awareness about data privacy and security issues within the educational sphere.

Commonsense Media stands out among them, having meticulously vetted over 200 EdTech tools in the past 5 years. Utilizing an extensive questionnaire comprising 150 questions, their team, alongside legal advisors, rigorously examines the privacy policies of EdTech platforms and assigns ratings on a privacy scale ranging from safe to risky.

Similarly, **Parents for Privacy** has introduced a tool designed to evaluate the student data privacy measures of all states in the country. Additionally, other initiatives such as **The Ethical Framework for AI in Education** focus on assessing ethical AI practices in education settings. Websites such as the **Student Data Privacy Consortium** offer templates for Data Privacy Agreements (DPAs) between schools and vendors, facilitating smoother collaborations while addressing privacy concerns.

Limitations:

- Complexity and Time-Intensiveness: Many of these tools are highly intricate and have undergone years of compilation. Their complexity and time-intensive nature make them less readily applicable or usable in school contexts.

- Lack of Focus on Emerging Technologies: Some tools fail to specifically address privacy concerns related to emerging technologies like Gen AI, potentially leaving gaps in privacy protection measures.

- Uncertain Adoption: The adoption of these tools by schools and educational stakeholders remains uncertain, raising questions about their effectiveness in improving student data privacy practices at scale.

EdTech Provider Data Privacy Practices:

EdTech vendors are increasingly prioritizing data privacy measures on their platforms, with several practices emerging from interviews with Gen AI EdTech vendors:

- Cautionary Measures: Many organizations among the ones interviewed are adopting cautionary measures such as data anonymization, secure cloud practices, and robust password protection to safeguard student data.

- Privacy Principles: While some vendors have explicit privacy principles publicly available on their websites, others do not. However, all practices are self-regulated, lacking government regulations or guidelines on required privacy policies.

- Data Protection Efforts: Vendors recognize the importance of protecting student data and are implementing measures to ensure the clarity of data usage agreements and the purging of unnecessary data from external APIs.

- Balancing Data Collection and Risk: Striking a balance between collecting large amounts of data to improve the tool's personalisation while mitigating the risk of exposing data to higher threats remains a challenge for many vendors.

- Parent and Teacher Awareness: Some vendors are actively informing parents and teachers about data privacy aspects during onboarding and ongoing support. However, the effectiveness and utilization of these services by teachers and school staff are unclear.

- PII Rejection Processes: Certain organizations claim to have processes for automatically rejecting Personally Identifiable Information (PII) entered by students. However, upon further inquiry, clarity on these processes is lacking, with some vendors stating that they are under review.

Limitations:
While EdTech vendors are making strides in enhancing data privacy practices, several limitations persist. Self-regulation without government guidelines may result in inconsistencies in privacy policies across platforms.

Challenges remain in balancing data collection for tool improvement with the risk of data exposure. Lack of clarity on PII rejection processes and uncertainty surrounding the effectiveness of parent and teacher awareness efforts highlight areas for improvement in data privacy practices within the EdTech industry.

Other considerations and survey responses:

- Teachers are often experimenting on an ad-hoc basis with free AI tools in their classrooms, driven by a desire to enhance their teaching methods and engage students. However, this experimentation typically lacks guidance from formal procurement guidelines. With millions of classroom-centric tools available on the market, many of these tools may lack adequate privacy features, posing potential risks to student data privacy.

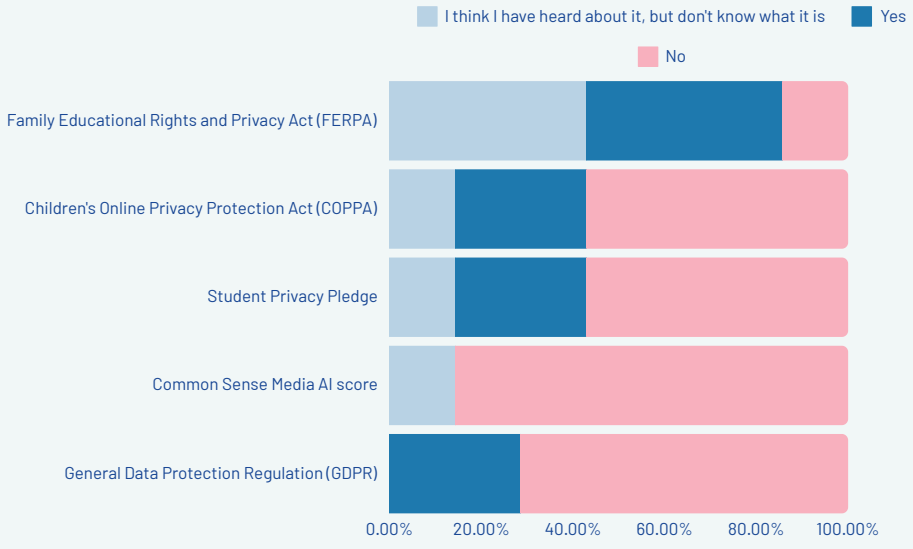
100 % of the respondents were not aware of the procedures or protocols that are in place at their school or district for responding to and reporting data breach incidents involving student information.

- Parents often find themselves overlooked in this landscape, unaware of the extent to which AI is integrated into their children's education. Many believe that schools do not utilize AI in the educational setting and remain oblivious to the potential data threats posed by AI technologies. Surprisingly, in the survey conducted, 43% of parents report that their children do not interact with AI either in school or at home. However, recent studies reveal a stark contrast, indicating that 46% of high school students engage with AI tools on a daily basis. This disparity underscores the critical need for improved communication and transparency between schools and parents regarding the use and implications of AI in education.

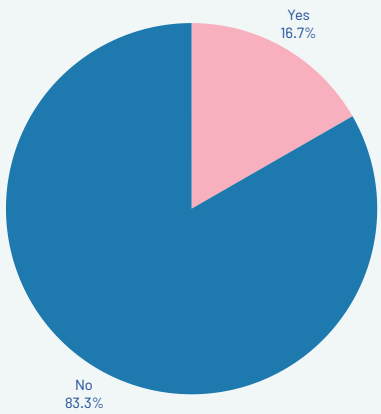
- We also surveyed parents and teachers to assess their understanding of student data privacy policies, resources, and safety measures. The results showed a need for better awareness and immediate implementation of protective measures. The findings are detailed here.

Parent/Teacher survey results:

Are you familiar with any of the following data privacy regulations/measures?



Have you undergone any trainings on how to ensure if the tool is adhering to safe data practices?



Need for increased and immediate data protection

Schools need easy-to-use tech tools to protect student data privacy, right now.

- Current tools are too complicated and take too long to navigate.
- We need faster ways for teachers, parents, and administrators to keep student data safe without getting bogged down.
- Everyone's input is important and should be considered: teachers know what students need for learning, parents know their kids best, and administrators make the decisions.
- Current policies are outdated and need to evolve to combat threats from tech advancements.

To effectively address the identified challenges, we have identified key criteria that any solution must meet to enhance immediate protection of student data. These criteria include:

Immediate reduction in data risk:

Every moment without comprehensive tools and guidelines leaves students vulnerable to potential harm(s) online. We cannot afford to wait for lengthy policy overhauls while students continue to interact with technology daily.

It is imperative to address this gap urgently to ensure the safety and well-being of students in today's digital age. The solution will be the stand-in while the policy change takes place ensuring immediate impact at the school level.

Cost Effectiveness

The solution should prioritize cost-effectiveness by maximizing security benefits while minimizing resource investment.

it should focus on scalable strategies that enable schools to achieve sustainable security enhancements without incurring excessive ongoing costs.

High practicality:

In a system where there is a paucity of time and resources, it is imperative that the suggested tools enable stakeholders to operationalize the recommendations with minimal effort keeping in mind the current practical landscape.

This tool will ensure that the suggestions are rooted in reality and support the stakeholders rather than becoming a burden.

Long term relevance

In an ever-evolving landscape of technology, where advancements occur rapidly, it's essential for solutions addressing data privacy to remain relevant over time.

The solution should aim to anticipate future technological developments and adapt accordingly, ensuring its effectiveness doesn't diminish as new technologies emerge.

Proposed solutions

Based on the goals outlined earlier and a comprehensive review of literature and other resources, the following solutions have been identified:

1. An easy-to-use student security assessment tool : A questionaire for stakeholders to swiftly evaluate data safety measures, raising awareness and providing actionable insights for schools and EdTech providers. By focusing on immediate risk reduction, it identifies potential risks across platforms, empowering stakeholders to make informed decisions. With a student safety focus, the tool caters to all stakeholders, aiding in the vetting of AI-powered EdTech for home or classroom use. It offers flexibility for both thorough analysis and quick safety checks.

2. Knowledge reserve of informative videos or blogs and links to relevant documents: This would serve as invaluable resources for school stakeholders to enhance their awareness of data security measures when utilizing AI-enabled applications. While these materials aid in risk reduction, the challenge lies in incentivizing their utilization without a tool or metrics demonstrating the necessity for heightened awareness among teachers and parents. It is also crucial to note that these resources may quickly become outdated given the rapid pace of AI technological advancements and the influx of new AI platforms in the market.

3. Training for teachers, school-level actors, and parents : In-person training, while valuable, can be time-consuming and may not immediately lead to risk reduction. Similar to online information, generating interest or willingness to engage in such professional development processes would require highlighting the associated risks and demonstrating how attending a training session could significantly reduce exposure levels.

CHOOSING THE ALTERNATIVE

1. An easy-to-use student security assessment tool:

This measure would entail designing an edtech and school security assessment tool with questions for stakeholders to quickly check for appropriate measures of data safety and raise awareness and provide actionable insights for both schools and EdTech providers.

2. Knowledge bank of data privacy information

For this we would create a knowledge reserve of informative videos or blogs and links to relevant documents on security measures to be adopted in the school by teachers, school admin and parents.

3. Training for teachers, school-level actors, and parents

A third approach to reducing data security risks could be through in-person training sessions for all teachers.

Scale of 1-5, 1 being lowest , 5 being highest

Given the above analysis of the considered alternative solutions to the problem of increasing data security awareness among stakeholders, particularly regarding the usage of AI platforms, **we have decided that the AI data privacy tool would be the ideal first step in securing children's data**. It would also pave the way for other measures to be taken up in due course for further analysis by educational institutions if they feel the need, and RAISE can start providing this in a staggered manner. A tool could stimulate demand for such informative content by first raising awareness of associated risks, serving as a follow-up to the risk assessment tool. This approach aims to garner buy-in and attention for the training.

Consideration of benefit of the tool before the adoption of the risk framework.

Though the tool is designed to measure and examine the risk level of the EdTech platform, it is important to evaluate the tool for its benefits and determine if it is worthy of considering the risks, taking into account the user's risk appetite. If the tool is not beneficial, even a minimal amount of risk is not worth taking. However, in other cases, the tool may be highly beneficial, and the personalization capabilities may justify some risk in order to leverage the advantages of using the tool. This may be the case in situations where there is a constraint in the availability of teachers, and the AI tool may enhance the teacher's capacity to provide better learning opportunities for all children. The tradeoff of giving up some data in a cautious manner may be justified in such scenarios. We hope that users of this risk assessment tool will keep these tradeoffs in mind and be cognizant of them before utilizing the tool for procurement or comparative analysis

AI Data Privacy Tool

This AI Data Privacy Tool provides a comprehensive solution to safeguard student data in the dynamic landscape of educational technology. Covering four key domains—1. Ethical Data Collection and Usage, 2. Privacy Regulation Compliance, 3. Redressal Mechanisms, and 4. Update and Review Mechanisms—the tool ensures alignment with educational objectives, regulatory statutes, and swift resolution of data breaches.

It also offers stakeholder-wise guidelines to promote responsible data usage at all levels in the education system. Crafted to achieve four fundamental goals mentioned above, the tool aims for an immediate reduction in data risk, advocates for collaboration across functions to protect student data effectively, and prioritizes high practicality to facilitate the operationalization of data privacy measures with minimal effort.

Domains of the tool:

1

Domain 1: Transparency of Data collection

Ethical data collection and usage ensure that student data is handled responsibly, respecting privacy and maintaining trust between stakeholders.

2

Domain 2: Privacy regulation compliance

Privacy regulation compliance ensures that student data is protected in accordance with legal requirements, fostering trust and confidence among stakeholders.

3

Domain 3: Redressal mechanisms

The implementation of robust redressal mechanisms ensures that in the event of a data breach, the affected individuals receive timely support and appropriate action is taken to mitigate the impact.

4

Domain 4: Update and Review mechanisms

The establishment of update and review mechanisms is crucial for ensuring that data privacy policies remain relevant and effective in the face of rapid technological change.

DOMAIN 1: TRANSPARENCY OF DATA COLLECTION

Today's EdTech platform providers have the capacity to collect and store vast amounts of data, often surpassing the scope of traditional school records protected by FERPA. This includes the expansion to indirect and inferred data, which raises concerns about the ethical collection and usage of student information.

It's crucial to critically analyze whether the data collected serves the intended educational purposes and whether personally identifiable information (PII) is appropriately de-identified during storage.

Significance:

Ethical data collection and usage ensure that student data is handled responsibly, respecting privacy and maintaining trust between stakeholders.

By scrutinizing data collection practices, educators and parents can ensure that student information is used effectively for educational purposes while minimizing risks associated with data misuse or exposure.

Guidelines for stakeholders

School Administrators:

- DO request a comprehensive list of the data being collected by EdTech providers and inquire about its intended usage to ensure alignment with educational objectives.
- DO advocate for data minimization practices, encouraging EdTech providers to avoid collecting unnecessary data that may pose risks.
- DO enquire about the duration of data storage and ensure it is not retained indefinitely on third-party servers to mitigate privacy risks.
- DO verify the data protection agreement with third parties providing underlying models to prevent unauthorized data usage or retraining.
- DO ensure there are clear opt-out methods for data collection processes, respecting their right to privacy.
- DO verify if EdTech providers are vetted by third-party privacy assurance agencies for compliance with industry standards.
- DO ensure that you do not enter sensitive details such as PII when interacting with EdTech tools unless absolutely necessary for educational purposes.

Parents/Caregivers:

- DO inquire about the data being collected by EdTech tools used by your child's school and understand its purpose and storage mechanisms.
- DO advocate for transparency and accountability in data collection practices, ensuring that student privacy is respected.
- DO educate your child about the importance of data privacy and empower them to make informed decisions about sharing their personal information online.

Teachers:

- DO ensure that the data collected by EdTech tools aligns with educational objectives and contributes to student learning effectively.
- DO educate students about responsible data usage and the importance of protecting their privacy when interacting with technology.
- DO ensure that you do not enter sensitive details such as PII when interacting with EdTech tools unless absolutely necessary for educational purposes.

DOMAIN 2: PRIVACY REGULATION COMPLIANCE

Compliance with privacy regulations is imperative for all EdTech organizations to uphold the standards set forth by the Department of Education or the FTC. Aligning privacy policies with regulatory statutes is essential to safeguarding student data and ensuring transparency and accountability.

Significance:
Privacy regulation compliance ensures that student data is protected in accordance with legal requirements, fostering trust and confidence among stakeholders.

By adhering to established regulations, EdTech organizations demonstrate their commitment to ethical data practices and mitigate the risk of regulatory penalties or legal consequences

Guidelines for stakeholders

School Administrators:

- DO inquire if the organization holds FERPA certification, indicating compliance with federal regulations safeguarding student educational records. Ask if the organization subscribes to COPPA regulations, which govern the online collection of personal information from children under the age of 13.
- DO ask if the organization subscribes to COPPA regulations, which govern the online collection of personal information from children under the age of 13.
- DO enquire if the organization has committed to the Student Privacy Pledge, demonstrating their dedication to protecting student data privacy.
- DO verify third-party vetting by ensuring the organization has been certified by reputable agencies like iKeepSafe or FTC-authorized certification bodies.

Parents/Caregivers:

- DO educate yourself about relevant privacy regulations such as FERPA and COPPA to understand the importance of regulatory compliance in safeguarding your child's data.
- DO advocate for transparency and accountability in data privacy practices by asking EdTech providers about their compliance with regulatory statutes.

Teachers:

- DO familiarize yourself with privacy regulations relevant to educational technology, such as FERPA and COPPA, to ensure compliance in classroom practices.
- DO collaborate with school administrators to verify that EdTech tools used in the classroom adhere to regulatory standards and protect student data privacy.

DOMAIN 3: REDRESSAL MECHANISMS

In the realm of data privacy, despite diligent efforts, the risk of occasional breaches remains unavoidable. In such instances, having clearly defined and prompt redressal mechanisms becomes paramount to restoring trust and safety for all affected parties. This domain focuses on establishing effective protocols to address data breaches swiftly and transparently.

Significance:

The implementation of robust redressal mechanisms ensures that in the event of a data breach, the affected individuals receive timely support and appropriate action is taken to mitigate the impact. This not only fosters trust within the educational community but also upholds the integrity of data privacy policies.

Guidelines for stakeholders

School Administrators:

- DO ensure that the data privacy agreement with providers clearly outlines the responsibility and accountability structures in the event of data leakages.
- DO build awareness among stakeholders, including parents and caregivers, about the Student Privacy Policy Office's redressal mechanism for privacy breaches.
- DO establish a dedicated committee tasked with overseeing and managing incidents of data breaches effectively.

Parents/Caregivers:

- DO familiarize yourself with the school's student privacy policy and understand the redressal mechanisms outlined therein.
- DO report any concerns or suspicions regarding data breaches to the relevant authorities promptly.
- DO look for signs or warnings of potential data breaches, as timely reporting is crucial for mitigating risks and minimizing impact.
- DO reiterate the importance of protecting PII whenever students use any AI tools

Teachers:

- DO stay informed about the school's data privacy policies and procedures, including the steps to follow in the event of a data breach.
- DO encourage students to report any instances of data breaches or privacy concerns they encounter.
- DO report any concerns or suspicions regarding data breaches to the relevant authorities promptly.

DOMAIN 4: UPDATE AND REVIEW MECHANISMS

In an era where technology and education are intricately linked, schools must continually adapt to rapid technological advancements to ensure students are adequately prepared for the future. AI represents just one facet of the transformative potential of technology, in the so-called “fourth industrial revolution”. As schools strive to cautiously integrate these innovations into their educational frameworks, it becomes imperative to establish robust mechanisms for updating and reviewing data privacy policies in alignment with evolving technological trends.

Significance:

The establishment of update and review mechanisms is crucial for ensuring that data privacy policies remain relevant and effective in the face of rapid technological change. By regularly revisiting and updating policies, schools can proactively address emerging challenges and opportunities in the realm of educational technology while safeguarding the privacy and security of student data.

Guidelines for stakeholders

School Administrators:

- DO establish a regular cadence for the review of data privacy policies, ideally conducting reviews at least once a year.
- DO require EdTech providers to actively inform school authorities of any changes to data privacy and protection policies, ensuring alignment with school policies.
- Do organize data privacy workshops or provide professional development resources for stakeholders to stay updated on new developments and best practices..

Parents/Caregivers:

- DO stay informed about updates to the school's data privacy policies and understand how they may impact your child's education and privacy.
- DO advocate for transparency and accountability in the review and updating process of data privacy policies to ensure the protection of student data.

Teachers:

- DO participate actively in data privacy workshops and professional development opportunities to stay updated on new developments and best practices.
- DO incorporate lessons on data privacy and cybersecurity into classroom activities to educate students about the importance of protecting their personal information online.

The guidelines are intended to serve as principles for stakeholders to consider while engaging with EdTech platforms that utilize AI in the classroom and at home. Based on these guidelines, an interactive validity tool has been developed. This tool will offer users a comprehensive security score, which will be determined by both the security level of the tool itself and the security measures implemented by the school and school-level actors.

It is also serves as a nudge to the user to enhance their awareness levels based on the responses to the tool and hopefully urges them to seek out easy to access resources to get to a basic level of data privacy awareness and also serves as a message to edtech providers to make this knowledge easily available to build stronger trust among the users.

The tool can be accessed in the appendix and through the following link.

Along with the tool, there is a supplementary data sensitivity matrix attached in the appendix. This matrix can assist stakeholders in gauging the sensitivity level of the data they are handling while creating and analyzing the EdTech tool's data collection inventory .

To ensure that this framework is embedded within robust structures and associated with specific measures by all the concerned stakeholders, we propose the formation of a school-level committee with clear responsibilities in the next section.

Committee for the AI Data Privacy Policy Implementation

Establishing an effective AI privacy policy implementation committee requires attention to the key elements of people, processes, and policies. While tools can aid in developing robust policies and processes, the success ultimately hinges on the individuals responsible for their implementation.

Given the multitude of responsibilities already borne by these individuals, it is crucial to delineate specific roles and responsibilities for each stakeholder involved. Additionally, it may be necessary to leverage external resources to augment the expertise of the school team and ensure efficient utilization of time and skills.

To facilitate this, we will utilize the **RACI matrix** to assign roles within each domain to the respective stakeholders. This matrix serves as a guide and can be tailored to suit specific circumstances and requirements.

We have included parents, teachers, school admin and EdTech vendors in this matrix. While imposing direct accountability on EdTech vendors for student platform security may pose practical challenges, this matrix serves as a gentle push towards reframing the narrative. It encourages envisioning the ideal scenario where EdTech vendors prioritize student safety to cater effectively to a large student audience.

RACI matrix for implementation

Domains	Parents	Teachers	School Admin	EdTech Vendors
Domain 1: Transparency of Data Collection	**C/I**	**A**	**R**	**C**
Domain 2: Privacy Regulation Compliance	**I**	**R**	**R/A**	**A**
Domain 3: Redressal Mechanisms	**C/I**	**C/I**	**R**	**A**
Domain 4: Update and Review Mechanisms	**I**	**C**	**A**	**R**

R: Responsible (responsible for executing tasks)
A: Accountable (ultimately accountable for the completion of the task)
C: Consulted (provides input and feedback)
I: Informed (kept informed about progress and outcomes)

Below, we provide detailed explanations of the roles of each stakeholder on the RACI matrix. For each domain, we outline the actions taken by stakeholders, their impact, and the consequences of inaction.

Domain 1: Transparency of Data Collection:

Parents: Consulted/Informed (C/I) - Parents play a crucial role in understanding and communicating data collection practices to their children and should be consulted and informed about the final decisions.

In this scenario, they should be informed about the AI EdTech platform's data collection practices. This awareness can empower them to advocate for transparency and ensure that students' privacy rights are respected if the data collection process is vague. If the parents remain passive or uninformed, it could lead to misunderstandings and concerns among them.

Teachers: Responsible (R) - Teachers are directly involved in implementing data collection practices in the classroom and should ensure transparency to students.

Teachers should ensure transparency by explaining to students during the class, through a short lesson how their data will be used and collected and reiterate this frequently. This creates awareness and empowers students to make informed decisions about their digital footprint. Conversely, neglecting to address these issues could result in students using the AI platform without due diligence and compromising high sensitive data.

School Admin: Accountable (A) - School administrators are ultimately responsible for establishing transparent data collection practices throughout the institution.

They are accountable for overseeing the procurement process and establishing transparent data collection practices school-wide and hence must take all the necessary measures to ensure that the selected platform complies with privacy regulations and aligns with the school's values. The school's administrator's commitment to thorough review and accountability demonstrates the school's dedication to protecting student privacy. Failure to uphold transparency standards could result in legal and reputational repercussions for the school.

EdTech Vendor Representative: Consulted (C) - The EdTech vendor may provide input on transparency measures, given their expertise in technology and data management.

The representative from the EdTech company must be consulted for better understanding of transparency measures. They must provide information and relevant demos on how the platform collects and uses student data. Willingness to provide transparency measures reassures other school stakeholders about the EdTech company's commitment to data privacy. However, if they fail to address concerns or provide adequate information, it could raise doubts about the company's integrity and trustworthiness.

Domain 2: Privacy Regulation Compliance:

Parents: Informed(I) - Parents should be aware of policies ensuring that their children's data privacy rights are protected.

This empowers them to raise questions about how the school ensures compliance with privacy regulations when using EdTech platforms. Knowledge of policies such as the FERPA, COPPA and GDPR helps parents to confidently contribute to the conversation about student privacy protection.

However, if they are unaware of privacy regulations, it may lead to concerns such as ignorance or parents regarding policies, data misuse and erode trust between the school and parents.

Teachers: Responsible(R) - Teachers are responsible for ensuring compliance with privacy regulations when using EdTech platforms in the classroom.

By taking responsibility for compliance with privacy regulations, teachers create a safe learning environment where students' data privacy is respected. This might look like the teachers taking the responsibility to educate themselves and the students about policies that protect their privacy. Failure to comply could result in legal consequences for the teacher and undermine trust in the school's commitment to student privacy.

School Admin: Responsible/Accountable (R/A) - School administrators are responsible for ensuring that the EdTech vendors comply with regulations and accountable for the school compliance with privacy regulations governing the use of EdTech platforms.

It is ultimately the school admin's role to ensure that there are measures in place to vet EdTech vendors and ensure that they adhere to privacy laws. Additionally, it is the school's obligation to ensure clear structures and practices to reduce risk at a school level through appropriate training measures, awareness building initiatives and review mechanisms in the school, which can then be executed by teachers and other responsible staff in the school. Failure to do so could result in heightened data risk levels which could be easily avoided.

EdTech Vendor Representative: Accountable(A) - The EdTech vendor should be held liable for ensuring compliance with privacy regulations.

It is essential that the EdTech company takes privacy compliance seriously and has implemented robust measures to safeguard student data. They should provide details about the company's compliance procedures and offer to share documentation to demonstrate their adherence to privacy regulations. This can help them differentiate themselves as a highly security-conscious vendor and help build a wider and trusted market for themselves.

Domain 3: Redressal Mechanisms:

Parents: Consulted and informed (C/I) - Parents may provide input and stay informed on the establishment of redressal mechanisms to ensure that they are effective and responsive.

In the establishment of redressal mechanisms, parents play a crucial role as they are directly impacted by any breaches or issues related to their children's data privacy. Being consulted and informed allows parents to provide valuable input into the design and implementation of these mechanisms, ensuring that they are effective and responsive to the needs of students and families. This also makes them feel empowered and reassured that their concerns are being taken seriously. Conversely, if parents are not adequately consulted or informed, they may feel marginalized and distrustful of the school's commitment to addressing data privacy issues. This could lead to heightened concerns among parents and potentially damage the school's reputation in the community.

Teachers: Consulted and informed (C/I)- Teachers should be consulted and informed about redressal mechanisms to address privacy concerns raised by students or parents.

In the context of redressal mechanisms,

teachers are often the first point of contact for students and parents when privacy concerns arise. Therefore, it is essential to consult and inform teachers about the mechanisms in place to address these concerns effectively. By involving teachers in the process, schools can ensure that they are equipped with the necessary knowledge and resources to handle privacy-related issues sensitively and efficiently. If this is not done effectively, it could lead to teachers feeling ill-prepared to handle privacy-related issues, leading to delays or mishandling of complaints.

School Admin: Accountable (A) - School administrators should take the lead in establishing and managing redressal mechanisms to ensure they meet the needs of the school community.

School administrators must oversee the implementation of clear policies and procedures for handling privacy-related complaints, including designated points of contact, escalation protocols, and documentation processes. If school administrators neglect this, it can lead to a lack of clarity and consistency in addressing privacy concerns, potentially resulting in unresolved issues, legal liabilities, and reputational damage for the school.

EdTech Vendor Representative: Responsible (R)- Ideally, in the event of a breach, the EdTech vendor must take the responsibility to ensure that the affected parties receive appropriate harm reduction support and work with the school admin to ensure the protocols are adhered to.

The EdTech vendor should collaborate with the school administration to ensure that established protocols are followed. This entails promptly notifying the school about the breach, providing detailed information about the extent and nature of the incident, and offering guidance on mitigation measures to minimize the impact on students, teachers, and parents.

Additionally, they must take proactive steps to address any vulnerabilities or weaknesses in their systems or practices that contributed to the breach, implementing corrective actions to prevent similar incidents in the future. If the vendor representative fails to take responsibility or respond adequately to the breach, it can lead to heightened concerns among users and loss of confidence in the vendor's ability to protect data.

Domain 4: Update and Review Mechanisms:

Parents: Informed (I) - Parents should be kept informed about updates and changes in data security policies to stay aware of any modifications or improvements.

This includes regular communication from the school or educational institution regarding updates to privacy policies, changes in data handling practices, and enhancements to security measures implemented by the EdTech platforms used in their children's education. Informed parents are better equipped to monitor their children's online activities, recognize potential risks, and provide guidance on safe digital practices. Without this, it can lead to confusion, mistrust, and concerns about the school's commitment to safeguarding student data.

Teachers: Consulted (C) - Teachers may provide input and feedback on updates and reviews of data security policies to ensure they align with classroom needs and practices.

They can offer valuable insights into how certain policies may impact their teaching methods, student interactions, and overall classroom dynamics making it vital that they should be consulted and given the opportunity to provide input and feedback on updates and reviews of these policies.

Without their input, policies may fail to address the practical challenges and considerations faced by educators, resulting in implementation issues or compliance gaps.

School Admin: Accountable (A) - School administrators are ultimately accountable for updating and reviewing data security policies to address evolving threats and requirements.

As the individuals responsible for overseeing the overall operations and compliance of the educational institution, school administrators play a pivotal role in ensuring that data security policies remain up-to-date and effective. Without timely updates, policies may become outdated or ineffective in addressing new threats and technologies, increasing the risk of data exposure or unauthorized access.

EdTech Vendor Representative: Responsible (R) - EdTech vendors bear a significant responsibility to proactively update schools on any changes or

advancements in their products or services that may impact data security.

It is essential for vendors to stay abreast of emerging threats, industry standards, and regulatory requirements related to data privacy and security. If vendors neglect their responsibility to keep schools informed about data security updates or fail to provide adequate support and guidance, it can undermine trust, erode confidence, and jeopardize the vendor's relationship with educational institutions.

The tool combined with the implementation structure should help reduce the risk levels of using the EdTech applications in the school and ensure that the students are able to enjoy the benefits of the platform without being to weary about the data risks

Tool validity testing

To test the efficiency of the tool and ensure its viability for usage compared to other tools in the market, the team conducted a validity test by comparing the security scores with those obtained from other tools. For this purpose, two edtech platforms were selected: the Khan Academy Khanmigo tool and the ChatGPT tool, commonly used in many schools for educational purposes. To compare privacy tools, we looked at how the RAISE tool rated these platforms compared to Common Sense Media's ratings. Then, we analyzed the scores we obtained.

The RAISE tool initially evaluated Khan Academy and ChatGPT with equal weights for all questions, resulting in Khan Academy receiving a 54% Privacy score and ChatGPT a 27% Privacy score. However, this scoring didn't fully reflect the nuances of privacy concerns.

To address this, a series of weights were introduced based on the judgment of the importance of each question and its influence on overall security. This adjustment led to Khan Academy's score rising to 63% and Chat GPT to 30%.

These revised scores better captured the specific privacy landscape of each platform. Comparing RAISE's evaluations to Common Sense Media's assessments reveals interesting insights. Common Sense Media provided Khan Academy with an 80% Privacy score and ChatGPT with 48%. This disparity underscores the differing methodologies employed by each evaluation system.

RAISE takes a holistic approach, considering not only the platform's privacy policies but also factors like a school's readiness to handle privacy concerns. If information necessary for evaluation isn't readily available or requires significant expertise to interpret, RAISE may assign a lower score. This cautious stance encourages schools and edtech providers to prioritize transparency and robust data protection measures.

While RAISE may yield more conservative scores compared to other evaluation methods, its aim is to ensure that stakeholders err on the side of caution when it comes to safeguarding student data. This highlights the importance of transparency and accountability in the edtech industry, ultimately promoting a safer online learning environment for students.

	Khan academy	Chat GPT	Notes
RAISE tool	54% Privacy score	27% Privacy score	• This may not be an accurate reflection of security of tool • Tool agnostic indicator is separated out
RAISE Tool Weighted	63% Privacy score	30% Privacy score	• Weighted tool has higher score • Considers student level easy to find indicators, which may be missing • Can include delphi method for better triangulation
Common Sense Media	80% Privacy score	48% Privacy score	• In depth analysis with many more factors like fairness of data usage, and transparency • 5 year endeavour with detailed examination of tool

Conclusion and next steps

This tool aims to be easily accessible and user-friendly for school teams and individuals interested in using AI EdTech platforms in schools, classrooms, and at home. It's designed to be open to improvement regarding the questions, weights, and calculation methods used to generate scores.

The goal is to enhance students' data privacy through a simple yet powerful tool, catering to stakeholders with limited technical knowledge of data security. It also serves as a message to EdTech providers, urging them to prioritize data privacy practices and transparency measures on their websites. This ensures that school-level stakeholders can quickly access privacy-related information and assess platforms for trustworthiness without feeling overwhelmed.

The intention is for this tool to be applicable to all AI EdTech platforms in the market and remain relevant for years to come with minimal updates. This allows school stakeholders to continue using the tool for procurement and usage decisions, even as new technologies emerge.

We plan to complement the tool with training materials such as videos and in-person sessions to increase awareness. However, the tool will remain the initial step in fostering the need for privacy measures and ensuring that all stakeholders are involved in the discussion.

Appendix A: AI Data privacy Tool

High Priority/ Must have:/ Quick check/ important checks	High security	Medium security	Low security
Is the data being collected aligned to the educational outcomes?	Yes	Apart from educational outcomes, some of the data being collected is to ensure smooth functioning of the tool	Data being collected has no relation to the educational outcomes or better tool functionality
Is the tool certified for adherence to privacy regulations such as the FERPA and COPPA by third party security as a service companies such as Ikeep safe, etc.	Yes, they have certifications of COPPA and FERPA		They do not have any certification
Has the tool making organisation subscribed to the Student Privacy Pledge?	Yes, they are subscribed		No they are not subscribed
How long is the data retention period by the tool?	<=3 months	More than 3 months	There is no information available to verify this
Are there clear opt-out methods for students from their data being collected and are they aware of this? Are there clear data deletion methods for the students and are they aware of it?	Yes, there are clear mechanisms for opt out and deletion of data and there are clear awareness programs around it.	There are some settings for opting out of some services and data collection	No, there are no clear mechanisms around opt out or deletion
Does the tool have clear mention of not using student data for commercial purposes such as targeted, behavioral, or personalized advertising?	Yes, they clearly mention that the data will not be used for targeted advertising.	The policy vaguely alludes to not using the data for advertising purposes	No, there are no mention of whether the data would be used for advertising purposes or not.
Does the tool clearly mention that the data will not be used to retrain the model?	Yes, the tool explicitly states it won't use data for re-training or only uses school-level data for re-training.	They clearly state that the tool uses data to retrain the model and offers straightforward opt-out options.	No, there are no mention of whether the data would be used for re-training purposes.

In Depth analysis	High security	Medium security	Low security
Does the tool have mechanisms to reject the entry of PII	Yes, the tool detects PII and alerts the user when any such data is entered.		No the tool does not have any such capacity
Is there a clear data privacy agreement with the organisation that specifies the responsibilities of the organisations in case of a data breach or unhealthy data practices?	Yes, there exists a clearly outlined document detailing the responsibilities of all parties in the event of improper data handling practices.	There are some vague policies of data breach and redressal mechanisms	No, there is no clarity on the responsibilities of all parties in the event of improper data handling practices.
Do you have access to the Data Privacy Agreement(DPA) that the tool has with the third party providing the API? (only during conversation)	Yes, the organisation was very transparent about this	The organisation was able to reveal certain parts of the agreement	There is no information regarding the DPA
Tool agnostic assessment:	**High security**	**Medium security**	**Low security**
Are there awareness building processes / classes for students on what constitutes as PII data? Are they aware of how they can protect their PII?	Yes		No
Is there a clear oversight committee for procurement related decisions in the school?	Yes, we have representatives from the parent, teacher and School admin community that are part of the oversight committee for procurement.		There is no oversight committee
Are you aware of the procedure in the case of a data breach?	Yes		No

Is there a clear process on mechanisms for reporting to the Student Privacy Policy Office at the Department of Education in the event of a data security issue?	Yes, specific members of the oversight committee have been identified to report such incidents to the concerns authorities.		No, there is no clarity on the specific responsibility of the committee in the event of a data security issue.
Are school level stakeholders aware of the FERPA and COPPA regulations and your rights?	Yes		No
Are there clear procedures for review of the tools' privacy policies and the school's privacy policies on a regular basis?	Yes, there is a clear policy in place to review yearly	There is no clear policy but reviews take place on an ad hoc basis	There are no review processes
Have you undergone any trainings from the school or the education department on data privacy protection?	Yes		No
Are you informed about the school's AI tool procurement policy?	Yes		No
Does the school maintain a list of the technologies that have already been formally approved for use with students in a readily available format for teachers /parents to look up	Yes		No

Appendix B: Data Sensitivity Matrix

To effectively manage data security, it's imperative to begin with a comprehensive data or directory inventory. This involves identifying and cataloging all data types collected by EdTech platforms. Once inventoried, these data types should be classified into various categories based on their characteristics and purposes. Subsequently, they should be assessed for sensitivity levels, considering the potential impact of exposure or misuse. This process enables a clear understanding of the level of exposure each data type poses, facilitating targeted security measures to safeguard student and school information.

Following NIST data classification principles, we have categorized the data types collected by EdTech platforms into high, medium, and low sensitivity levels. This classification is based on the potential severity of damages to individual students and schools in the event of malicious activity.

Sensitivity Level	Type of data
High Sensitivity	**Personal Identifiable Information (PII):** This includes information such as name, address, date of birth, and social security number, which directly identifies a child and poses significant risks if exposed or misused. Any unauthorized access or breach of PII can lead to identity theft, fraud, or other serious consequences. All other data types, when presented along with PII, become highly sensitive data. **Biometric Data:** Biometric data, including fingerprints, voiceprints, and facial recognition data, is unique to individuals and can be highly sensitive. However, in the context of child data protection, the collection and use of biometric data are less common compared to other types of data. Therefore, while biometric data is inherently sensitive, its prevalence in child online data may be lower, resulting in a relatively lower sensitivity level.
Medium Sensitivity	**Sensitive Personal Information (SPI):** While SPI may not directly identify a child, it comprises sensitive data such as health information, religious beliefs, and sexual orientation. Although not as immediately identifiable as PII, SPI can still be highly sensitive and may cause harm if disclosed or misused. **Behavioral Data:** Behavioral data, including browsing history, search queries, and interactions with online content, can provide insights into a child's preferences, habits, and interests. While not inherently identifying, this data can still be sensitive and may present risks if accessed or used without consent. **Academic Performance Data:** Students' academic performance data, including grades, test scores, and learning progress. **Geolocation Data:** Geolocation data, such as GPS coordinates or IP addresses, provides information about a child's physical location. While the disclosure of geolocation data may raise privacy concerns, it typically poses lower risks compared to PII or SPI. However, precise geolocation data may still warrant higher sensitivity levels due to potential safety implications.
Low Sensitivity	**Generic Chat Data:** Prompts and chat data from students' interaction with chatbots could be low sensitive if it is free from PII and other identifiable information.

Bibliography and Resources

Data privacy agreement template from student Data Privacy Consortium

A standard template for schools to use in the process of creating data privacy and usage agreements with EdTech tool developers during the process of procurement.

Common Sense Media-State of Kid's privacy

This is an in depth and comprehensive analysis of the data hygiene and safety practices of the top 200 educational/ child facing platforms. It covers many domains of data hygiene that can be incorporated into this research project. Additionally, it will inform this project immensely as it sheds light on the adherence to the data privacy statutes that have been mandated by the federal government.
This evaluation process took upwards of 5 years to complete, with the support of many experts, it would be demanding of school level stakeholders using this as if for their decision making. The stakeholder's decision making process would need a highly concise with only a few things that are in the purview of the school stakeholders

Ready for School Recommendations for the Ed Tech Industry Protect the Privacy of Student Data

This report from 2016 by the office of attorney general of California outlines the issues related to ed-tech data privacy and provides recommendations for EdTech platform creators on ensuring better data practices while designing the platform.

Student Privacy Pledge:

The student privacy pledge is a set of commitments that service providers voluntarily promise to comply with to ensure student privacy on their platforms. The Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) compiled the list of commitments in 2020 based on federal regulations that protect student safety.

AI Guidance For Schools Toolkit by Teach AI of Code.org

The document provides a comprehensive set of guidelines for schools to adopt to ensure the best usage of AI platforms at the school level. They briefly also mention privacy measures but do not elaborate on how parents and teachers can look for these indicators of strong privacy measures on these EdTech platform websites while deciding what to procure.

University of California AI Working Group Final Report

This document outlines the University of California's Responsible AI Principles, which serve as a comprehensive framework guiding the procurement, development, implementation, and ongoing monitoring of artificial intelligence (AI) technologies across its various campuses. These principles are designed to ensure that AI initiatives within the University uphold ethical standards, promote transparency, protect privacy, mitigate bias, and prioritize the well-being of all stakeholders.

K-12 Generative AI Readiness Checklist October 11 2023

The report by the Council of the Great City Schools (CGCS) and CoSN (Consortium for School Networking) worked in partnership with Amazon Web Services (AWS) details out a set of questions that need to be asked and answered to ensure readiness of the state district to implement AI technology in the classroom. It includes sections specific to data readiness and security readiness touching upon themes of data privacy and transparency practices.

The 2019 State Student Privacy Report Card

The document by Parent Coalition for Student Privacy provides an extremely detailed grading of all states in the country on the basis of a comprehensive matrix of categories and subcategories involving scores for each domain including compliance to federal data protection regulations and other data safety methods.

Michigan Education Technology Leaders Quick Self-Audit Data Collection Tool

An easy to use document of risk controls for edtech leaders in the state to audit data collection by EdTech Tools.

The Ethical Framework for AI in Education

The framework emphasizes the importance of considering ethical considerations, stakeholder perspectives, and practical applications to ensure responsible and beneficial integration of AI technologies in education. It presents six overarching questions to guide further research and discussions on the ethical implications of AI in education. These questions focus on stakeholders' perspectives regarding the risks and benefits of AI in education, strategies to resolve tensions between risks and benefits, and practical implementation of ethical principles in the context of AI use in educational settings.

The K-12 Privacy Policy Guide *How to Quickly Spot Red Flags*

A quick guide with a list of “red flags” to look for in the privacy policies of EdTech platforms creates by the Public Interest Privacy Center to safeguard student data.

Acknowledgements

Contributions of numerous individuals in the Goldman School and at MIT RAISE have been instrumental in shaping this project. I am deeply grateful to all those who shared their time to make this project possible.

A big thank you to Professor Andrew Reddie for his guidance and support as my capstone instructor this semester.

I am also immensely grateful to Mary Cate Gustafson-Quiett and Eric Klopfer at the MIT RAISE lab for their wonderful mentorship and help in shaping and constantly supporting this work.

I deeply appreciate all the interview participants, survey respondents and expert advisors. Your inputs have been extremely valuable to this project.

Thank you to all the professors who have provided skills and teaching throughout my time at Goldman that have informed my approach to this project.

I would like to thank my capstone colleagues for your inputs in improving my project and report through out the semester.

Lastly, a huge shoutout to my family and friends for cheering me on through this learning journey.