Securing Student Data in the Age of Generative AI

A Tool for Data Privacy Enhancement in K12 Schools

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 paper 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 the white paper - “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 proposal 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 of ensuring safe data practices while onto the generative AI based EdTech platforms to minimize data collection rather than placing it on individuals to navigate complex legal documents.