VIEW POINT

EDUTECH SERVICES AND DATA PRIVACY

Abstract

Efforts to make educational practices more efficient, a shift towards digital channels, and circumstances of the Covid-19 pandemic have resulted in edutech application adoption in schools increasing by 99% since 2020. However, as these applications rely on data to offer quality education and timely intervention to students and ensure accountability, concerns for data privacy in education and edutech are also becoming prominent. Some data protection and education risks include data misuse by vendors or schools. The risks could also come in the form of malicious third-party applications or security protocols, the infrastructure of the edutech platforms, data leaks, and cybercrime. Although these risks can potentially leave student data vulnerable for malicious agents to exploit, understanding how to identify and mitigate these risks can help you ensure your students' data is safe and they can get the most out of various edutech applications.

Infosys®
Navigate your next

The field of education technology is vast, and aims to increase the effectiveness and efficiency of contemporary educational practices. If you consider this aim of edutech, you can trace its roots as far back as cave paintings that imparted the knowledge of life to the next generations or the educational films in the early-to-mid 1900s. The edutech as we know it has its roots in the late 1990s when the World Wide Web had reached mainstream awareness and made presentation-based technology accessible to the masses. And what started as educational documentaries, PowerPoint presentations, video courses, and webinars have now evolved to include gamification, artificial intelligence, augmented reality, and virtual reality to make education more effective.[1][2]

Years following the Covid-19 pandemic have made classroom tech and edutech so mainstream that it is impossible to imagine a modern educational institution that uses zero edutech applications. As a result, the global edutech industry is now worth $340 billion and will reach $605 billion by 2027. And as students and educators alike become more comfortable with technology, the use of edutech applications in schools has increased by 99% since 2020.[2] However, the concerns for data privacy in education and data protection for students accompany this widespread acceptance of edutech in modern schools.

Edutech in schools and data collection

If you are a student today, it is impossible to not rely on digital technology, from student intake and storing student information to accessing class resources, completing homework, or accessing your grades. At these touchpoints, a business extracts, collects, and repurposes data behind the scenes. This has given rise to discussions around data protection in education and implementing efficient data privacy standards to protect students.

And even if we move away from the number one goal of any business – profitability – edutech companies rely on data collected from student and faculty interactions to refine their products, offer personalised study plan to meet individual student needs and ensure student accountability. With data driving precision, early intervention, and accountability in edutech, it is almost impossible for students to opt out of data collection. This makes the discussion around data protection and education even more important as the vulnerable students are the most affected in this case.[3]

Types of student data

Edutech platforms and applications collect a lot of data to build a roadmap of a student's progress and build personalised intervention for a student's individual needs. The five types of student data an edutech platform and the school administration collect and store are:[4]

1. Personal data: This includes the personal identifying information about the student, including name, address, date of birth, age, ethnic background, ID number, and much more.

2. Academic data: Academic data is the key point of interest for edutech applications as it allows them to monitor and track a student's progress. This includes the enrolment details, weekly schedule, attendance records, report cards, and grades of the individual students.

3. Health data: Health data is necessary to address any medical emergencies on the school grounds or make appropriate accommodations for a student's needs. This includes medical history, chronic conditions, learning disabilities, and insurance details.

4. Parent data: Along with students' personal information, schools also need access to patent information, which includes parents' personal identifying information, banking information (credit or debit cards), and emergency contacts.

5. Third-party data: Third-party data includes usernames, passwords, student progress, and metadata of the different learning apps the school uses. This information helps monitor student activity, ensuring they adhere to school policies, and extend technical support to the students when needed.

Each data type has different utility and importance when it comes to edutech platforms and applications. However, without appropriate data privacy protocols, schools may leave student information vulnerable to attack or misuse.

Analytics will empower employees.

The first step in making data protection and data privacy in education is to understand the key data privacy risks facing the edutech platforms and the potential strategies to identify and mitigate any threats to student data. The eight major edutech data privacy risks are:[4][5]

1. Vendor misuse: One of the biggest data protection concerns among students, parents, and policymakers is how the edutech vendors collect and use the data. The type, nature, and sensitivity of the data may vary depending on the vendors and the services they provide. Although student data privacy laws restrict what information vendors can collect and store, there is still the possibility of vendors using student data for advertising or selling this data to external parties for revenue. Understanding the privacy policy of individual vendors and checking their adherence to data governance policies may be a good starting point to mitigate this risk.

2. School misuse: Pervasive use of student surveillance technology, in physical school environments and within edutech applications is a great cause of concern for many students and their guardians. This can potentially help schools monitor students, offer timely intervention, and detect any harmful behaviour. However, such technology can also severely compromise the privacy of the students or can facilitate targeting minority students. Here, the schools need to be accountable for striking a balance between student cyber safety and school policies while communicating clearly with students, parents, and guardians about school policies and processes.

3. Edutech app security: Modern schools use multiple technologies and edutech apps to give students an all-around education and experience. A security breach in any of these apps can seriously compromise student data, making your data security systems as strong as your weakest link. The obvious mitigation strategy here is to vet the edutech applications' data security and governance policies to ensure data protection in education.

4. Insecure data transfer and storage: An extension of the third point, insecure data transfer between different edutech apps or lacking security measures for data storage can compromise data privacy in education. Here, vendors are responsible for incorporating stringent data security protocols on infrastructure and application levels to mitigate this risk.

5. Risky OAuth access: Open standard authorisation frameworks like OAuth facilitates the free movement of data and controls between domains like Google or Microsoft 365 and third-party apps. OAuth can circumvent traditional security controls and, thus, can threaten data protection for students. Although its primary use is to facilitate easy login between various applications, it may also allow access to other information like contacts, profile data, photos, documents, and more. Being vigilant when granting access permission can be a great way for students to effectively mitigate this risk.

6. Insider data leaks: Either intentional (malicious) or unintentional (accidental) data leak is one of the biggest threats to a school's data privacy. Setting up controls through your security systems and educating the users on data privacy processes is a two-fold way to address this risk.

7. Malicious third-party applications: Malicious third-party apps can trick users into granting access permissions by posing as legitimate edutech apps, fun games, or lifestyle apps. User education and vigilance are two key strategies to identify and mitigate this risk to student data.

8. Cybercrime: Cybercrime is the biggest threat to data security in any sector, and edutech applications are no exception. Activities like data breaches, ransomware attacks, phishing campaigns, and account takeovers can not only put school data privacy at risk but can threaten students and parents as well. A stringent cybersecurity strategy along with cybersecurity and data safety training for staff and students, can help mitigate this risk.

Data privacy and student data security in edutech

Data is the foundation of quality, precision, and accountability in edutech applications. And securing this data is critical to protecting the students from data loss and any resultant negative consequences. Student data privacy laws offer a framework for data privacy in education. However, policymakers, school leaders, staff, students, and their parents (and guardians) need to understand the potential security risks for data protection and education technology. This can help them effectively identify and mitigate them while working with the vendors or educating the users to improve security infrastructure and protocols in edutech apps.[5]

Conclusion

Selecting a trustworthy and secure third-party edutech vendor is integral to understanding how different businesses are accessing, storing, using, and sharing student data, thus, making an informed decision about selecting the edutech services. Leading BPM organisations can make it easier for you to access secure cloud-based learning solutions that are secure, efficient, and offer a rounded learning experience to your students. Thus, you can be sure your students are getting the best possible education without worrying about data privacy and data protection in education.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping **organizations with intuitive decision**-making automatically at scale, actionable insights based on real-time solutions, anytime/ anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next