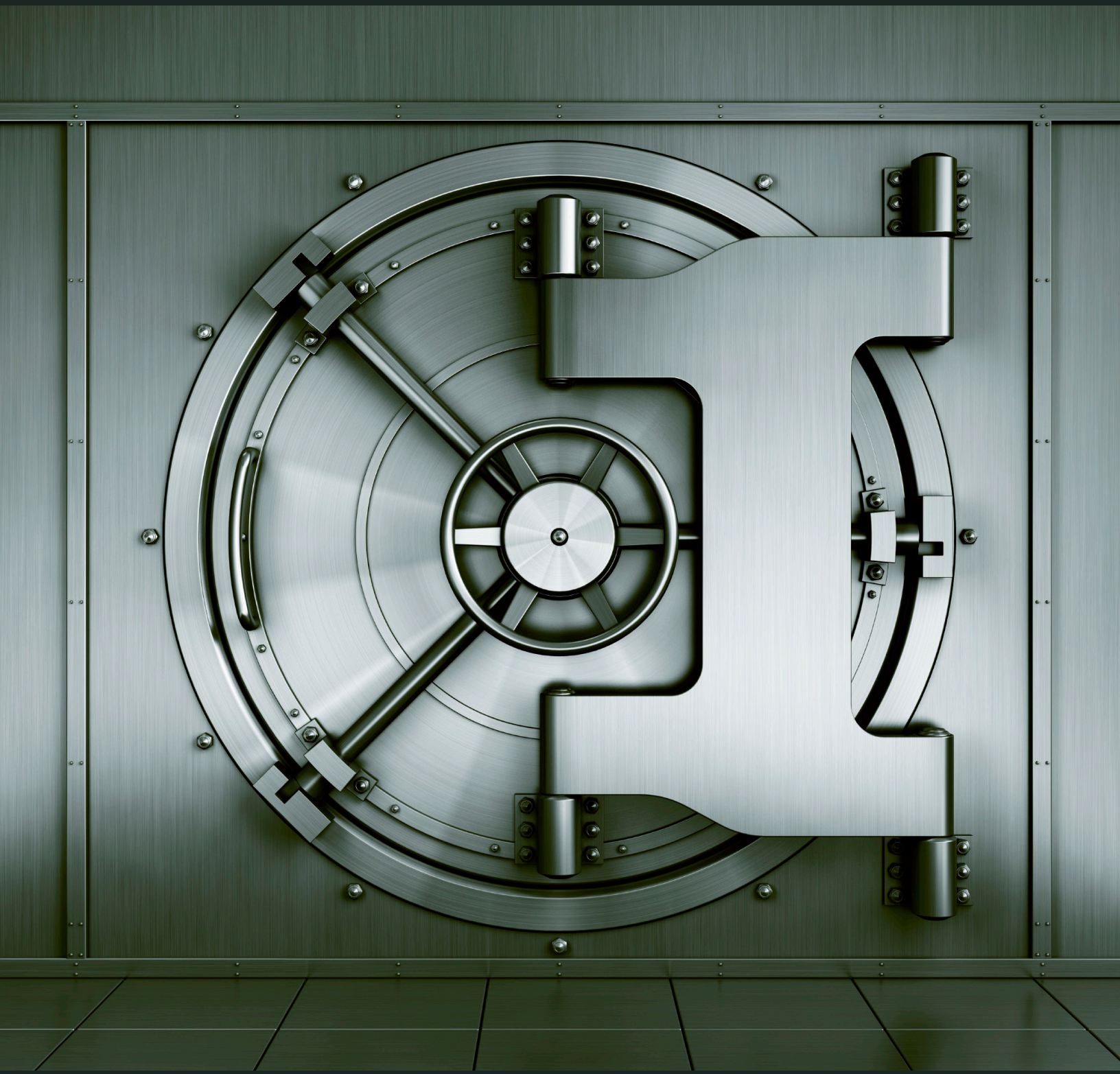
Your Data in Your Control

How Your Student Data is Staying Safe



Jupiter Ed

The privacy and security of student data in under scrutiny in the U.S., partly due to the growing use of cloud computing. Businesses have long used cloud computing for its flexibility and cost effectiveness in storing and sharing large volumes of data. The education sector has now made the same transition, which raises questions of who has access to what data, and for what purpose.

A 2014 report by McKinsey & Company stated that the education sector could benefit the most from the free exchange of data. The report stated that the exchange of this data could add as much as $1.2 trillion to the economy through more efficient, effective instruction. Along this same money-saving vein, using cloud-based data storage keeps schools from having to spend large amounts of money on paper and other supplies and be used for the storage of student information. Cloud services also save memory and disk space on computers.

With more student data transitioning from local school district servers to third-party services in the cloud, schools and parents are increasingly concerned about data leaking into the wrong hands, or being used for inappropriate purposes without consent. There has been increasing demand for guidelines and regulations to ensure student data is kept private and secure.

On January 12, 2015, President Obama announced he will propose a law called the Student Digital Privacy Act. This legislation would prohibit companies from selling student data to third parties, and from using information schools collect to engage in targeted advertising. If this bill passes, parents and schools will feel further at ease when dispensing necessary information about their students.

The Student Digital Privacy Act is not the first act that protects student data. The U.S. Department of Education's 2013 National Education Technology Plan proposed ways of using data from online learning systems to improve instruction. The plan encouraged education institutions to begin using analytics to improve academic outcomes and increase student grades and retention.

In 1974, the Family Educational Rights and Privacy Act (FERPA) was created to protect the privacy of student education records. It provides parents the right to inspect and review their child's education records maintained by the school. Once a student turns 18 or attends a post-secondary school, these rights are transferred to the student. Schools must have written permission from parents or eligible students before sharing his/her education records with third parties. FERPA also protects information from misuse or inappropriate purposes. Since this 1974

law was written before the advancement of computers, the Department of Education has more recently written guidelines on how FERPA applies to the student data stored and managed in this new technology.

Another relevant privacy law is the Child Online Privacy Protection Act (COPPA). This Act applies to any websites or online services that collect, use, or disclose any information of children under the age of 13. COPPA more thoroughly details the guidelines that website operators must follow. For example, they must provide a clear and complete privacy policy, maintain the confidentiality of the information they collect, minimize the retention period for children's information to as long as is necessary and then delete it accordingly, and must get parental consent before collecting private information online directly from their child. They must also provide parents access to the information collected on their children, and allow parents to withdraw permission from future collection of their children's information. (This law does not govern data collected from parents or from other schools.)

Recently, the Center on Law and Information Policy at the Fordham University School of Law conducted research on the privacy of student data in the cloud. The study mainly focused on K-12 public education and how schools address the privacy and security of their students while moving their services to the cloud. Some of their key findings indicate that about 95% of school districts rely on cloud services for managing classroom activities, student education, and many other aspects. The research found that, unlike Jupiter Ed, the majority of the other cloud service providers do not address parental consent or access to student information in their privacy service agreement letters. Many of the other K-12 providers did not guarantee student data security, and they sometimes even allow third-party vendors to access sensitive data.

In this age of big data, it is the responsibility of schools and cloud service providers to work together to protect the privacy rights of students. Students, parents, and administrators deserve complete transparency regarding data handling and security practices of cloud service providers.

Jupiter Ed and Your Data

Jupiter Ed is in full compliance with all the FERPA requirements, qualifying under the "School Official" exception (CFR) §99.31(a)(1), because your data is in your direct control, and used only for legitimate educational interests and functions that the school's own employees normally perform.

FERPA does not require parental consent for such use. Jupiter Ed does not share any personally identifiable information (PII) with any third party, or use it for non-educational purposes (spam, targeted ads), except when a school exports or enables their student data (directory information) to be sent to third-party software, such as a curriculum web application.

Under Jupiter Ed's Terms of Service, the school may use student information only for educational purposes. Instructors enter the student's grades and personal comments, which is available only to the instructor and other staff in the same school district, depending on the permission settings set by the school. Students and parents may also see their information online, but not of other students. Personal information may be seen by Jupiter Ed support staff when you ask for technical support. If the school asks students under 13 to provide their contact information online through Jupiter, the school must obtain the parent's consent as required by COPPA. To ensure privacy, students and parents must keep their passwords confidential and logout when done.

Jupiter Ed has several security features to protect the privacy of student data:

Encryption — Jupiter Ed uses TLS/SSL encryption. All passwords are salted and hashed using multiple algorithms for maximum security.

Network Security — We have proven defenses against malicious attacks, like cross-site scripting (XSS), SQL injection, brute force, phishing, distributed denial of service (DDoS), and other exploits. Due to our excellent network security, we have never had a security breach.

Suspicious Activity — All logins are logged and cross-referenced to identify suspicious activity and alert you immediately by email.

Role-Based Security — Set custom restrictions for teachers, clerks, counselors, AP's, principals, TA's, substitute teachers, etc. to prevent them from seeing or changing certain data.

Backups — Our servers are backed up nightly to an off-site location, and they have redundant hard drives (RAID) so no data is lost in case of hardware failure. If anyone gains unauthorized access, you may selectively undo changes to grades and attendance without having to rollback the entire database.