PowerSchool

WHITEPAPER

K-12 Security Tips That Will Protect Student Data Today

September 2022

Contents

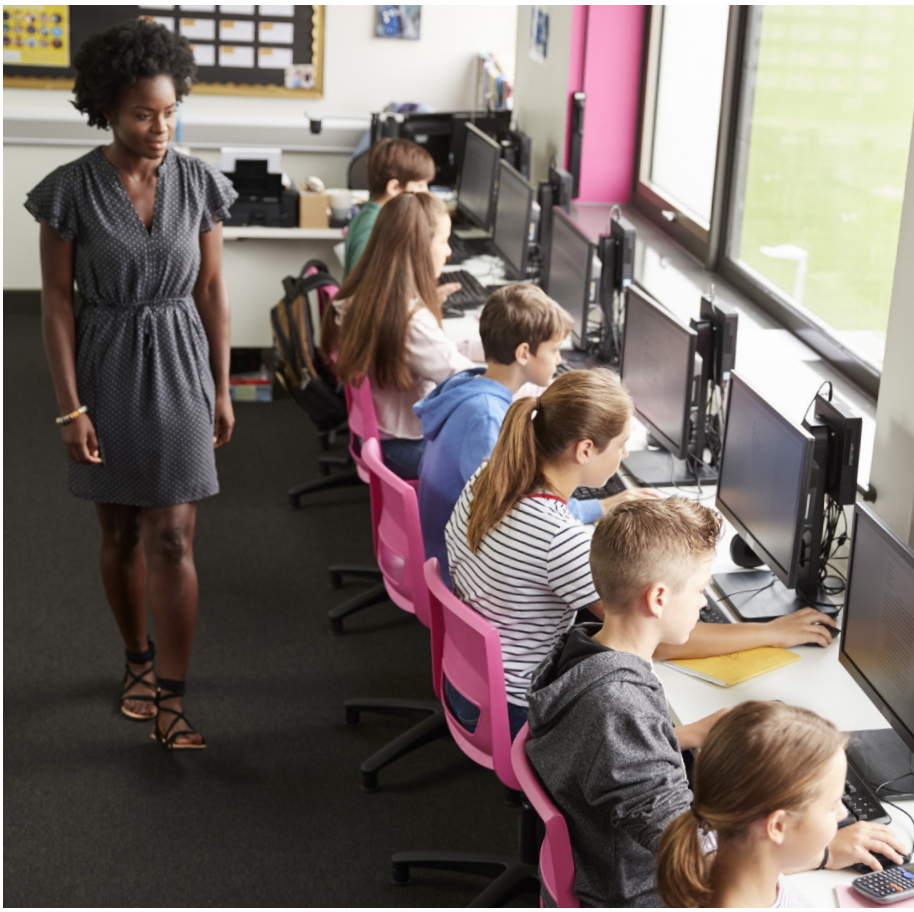
Data Security Impacts Everyone

We've all seen the headlines: *Apple Security Flaw 'Actively Exploited' By Hackers to Fully Control Devices*[1]*... Massive Data Leak Exposes 700 Million LinkedIn Users' Information*[2]*... Stolen Data of 533 Million Facebook Users Leaked Online*[3]*...*

Hackers have successfully attacked Amazon, Twitter, Google, Yahoo, and JP Morgan Chase, leaving more than one billion of their customers and their personal information vulnerable.

No one is 100% safe from cyber threats, and no company is off limits to hackers—including K-12 schools and districts storing sensitive student information. In fact, FBI reporting indicates an increase in ransomware specifically targeting K-12 schools.[4] Ransomware is now "the most common type of publicly disclosed cyber incident at U.S. schools," according to the K-12 Security Information Exchange.[5] In 2021, 67 ransomware attacks affected 954 colleges and schools, potentially impacting almost a million students.[6] Additionally, according to the 2022 Data Breach Investigations Report by Verizon Wireless, there were 1,241 incidents and 282 with confirmed data disclosure.[7]

The fallout? When hackers infiltrate a system, schools and districts suffer data corruption/manipulation, data loss, theft of sensitive Personally Identifiable Information (PII), impaired function, expenditure of resources, and ultimately, loss of trust over the long term.



Examples of Security Disasters & Breaches

NAME	YEAR	RECORDS	ORGANIZATION TYPE	METHOD
Cash App Investing	2022	8.2 million	Financial Institution	Inside Job
Florida Healthy Kids Corporation	2021	3.5 million	Healthcare	Hacked
Smile Brands, Inc.	2021	2.6 million	Retail	Hacked
Lakeview Loan Servicing	2022	2.57 million	Financial Institution	Hacked
Horizon Actuarial Services	2022	2.29 million	Consulting	Ransomware
Flagstar Bank	2022	1.54 million	Financial Institution	Hacked
Baptist Medical Center	2022	1.24 million	Healthcare	Hacked

80 percent of parents say they worry about their children's **privacy and security when using apps**

The effects from attacks on your district can be devastating. In 2022, a cyberattack on a leading provider of student-tracking software resulted in an enormous data breach. The attack affected the personal information of more than one million current and former students across dozens of districts, including New York City and Los Angeles districts.

Recovery of a single ransomware attack lasts an average of 287 days, "even when the victim organization believed it had secure backups in place prior to the attack," according to the IST Ransomware Task Force.[8] Depending on the type and severity of the cybersecurity attack, many districts have to recreate data, rebuild systems, and sometimes cancel classes, or days or weeks of school. And modern ransomware attacks often exfiltrate data, holding it hostage, and causing additional privacy and identity protection concerns and actions.

In a digital age with the heightened fear of cyber security threats, hackers, internet security breaches, encryption ransomware attacks, identity theft, and advertisers tracking browsing habits, the importance of data security is growing exponentially. Worldwide, there are more than five billion internet users and 4.62 billion (and counting) active social media users. In 2022, a staggering 95 percent of U.S. teens have a smartphone or access to one, and 46% say they're online "almost constantly," according to a Pew Research Center study.[9]

Understandably, parents are worried; in a Harris Poll survey, 80% of parents say they worry about their children's privacy when using apps, with 73% concerned about apps tracking their children's location.[10] Parents become even more concerned when national stories emerge such as government or private organization email leaks, or the 2,000+ students whose personal information was compromised at Colorado's Lewis-Palmer School District 38 because of a security breach to its student information system (SIS).[11]

The responsible, safe collection and management of student data has become essential to student success and has transformed the way we help guide and personalize learning in the 21st century digital classroom. Educators can view individual student performance over time, identify positive and negative trends, and make real-time adjustments to help keep them on track.

Technology facilitates transparent communication between teachers, students, parents, and administrators for a collaborative learning environment. Students can interact on a wide variety of digital devices, including mobile—with online content. Teachers can quickly and easily provide grades, assign lessons, view progress, and make comments, all with a few clicks from wherever they are connected.

Tips That Will Protect Student Data Today

In truth, every school district has its own unique system and technology peculiarities. So, it's unrealistic to provide a one-size-fits-all approach to securing student data. However, there are basic guidelines districts can use to make data safer and less susceptible to cyberattacks.

Ensure that only required information is collected

As a rule, only collect data that's required, and nothing more. Collecting a variety of student data is vital for personalized learning success. This includes **Personally Identifiable Information (PII)** that refers to any information that could potentially be used to identify an individual.

There is often a tendency to store various data types even when it's not necessarily needed. School districts need to evaluate the data being collected and ensure that there's a business justification for it.

While it's important to collect data such as first and last names, date of birth, student number and grades, administrators should consider if it's necessary to collect more sensitive information like social security numbers.

Encrypt sensitive data

Data encryption is the conversion or translation of data from a readable format into an encoded format which can also be accessed by authorized users with the correct decryption key. By encrypting data, you're helping to maintain the confidentiality of sensitive data by ensuring that only authorized district staff can access the information.

Basic Encryption Tips

- Districts should ensure that student data, while at rest and in transit, is **encrypted in accordance with industry-accepted standards**
- Transfer of sensitive data, across systems, should be done over **TLS 1.2**, which is the **highest standard technology** for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems
- Storage of sensitive data in repositories should be **encrypted using a minimum of AES-256 encryption**
- Stored backups should also be encrypted
- In addition to database servers, data stored on mobile endpoints and removable storage devices should also be encrypted

To keep student data more secure, school districts should follow these password guidelines:

1. Use a password that is at least **eight characters** long. Make it longer if it is an administrator account.
2. Avoid using dictionary words or passwords that are easy to guess, like your school mascot. **Use passphrases**—a sequence of words or other text.
3. **Never write passwords** on "sticky notes"
4. When available, use **multifactor authentication (MFA),** which requires more than one method of authentication from independent categories of credentials
5. **Avoid using the same password** across different systems as this could lead to a total compromise of all systems if one password is breached
6. When available, districts should implement **Single Sign On (SSO)** for easier authentication across systems
7. When available, use a robust **password manager** that allows you to have unique and complex passwords for each account you have

Keep systems updated

Vulnerabilities are security weaknesses in software/systems. Attackers target software vulnerabilities in order to compromise information systems of school districts. When exploited, the attacker can steal data saved on database servers, gain control of the district's network infrastructure or install a malware/ransomware. These weaknesses can be fixed by keeping the system patches up to date.

To ensure that data stored on such systems remain secure, school districts should implement an effective patching cadence wherein known vulnerabilities are fixed within a defined period of time (known as an SLA, or Service Level Agreement). While all patch updates may not be rolled out at once, you can set the priority based on the severity of the vulnerabilities.

Proper password management

Passwords typically act as keys to a safe box. Access to servers, systems, and network devices are often restricted with the use of passwords, making them a prime target for attackers. *(See the password guidelines section to the left.)*

Network defense and endpoint protection

Network protection helps reduce the attack surface of your district's internal and private network from external or internet-based events. It helps ensure that only authorized network requests are made and sent in and out of the internal network.

To improve the security posture, districts should implement security measures to guard against disruption or denial of service, degradation, or destruction. This includes the implementation of Next-Generation Firewalls (NGFW), Virtual Private Networks (VPN), Intrusion Detection/Prevention Systems (IDS/IPS), proxy servers, spam filtering, vulnerability monitoring, antivirus or anti-malware, among other security measures.

Dedicated information security resources

To help coordinate the implementation of your security program, it's a wise move to employ the services of dedicated information security personnel. While data security is a collective responsibility, dedicated resources are specifically saddled with the task of ensuring and enforcing that appropriate controls have been implemented.

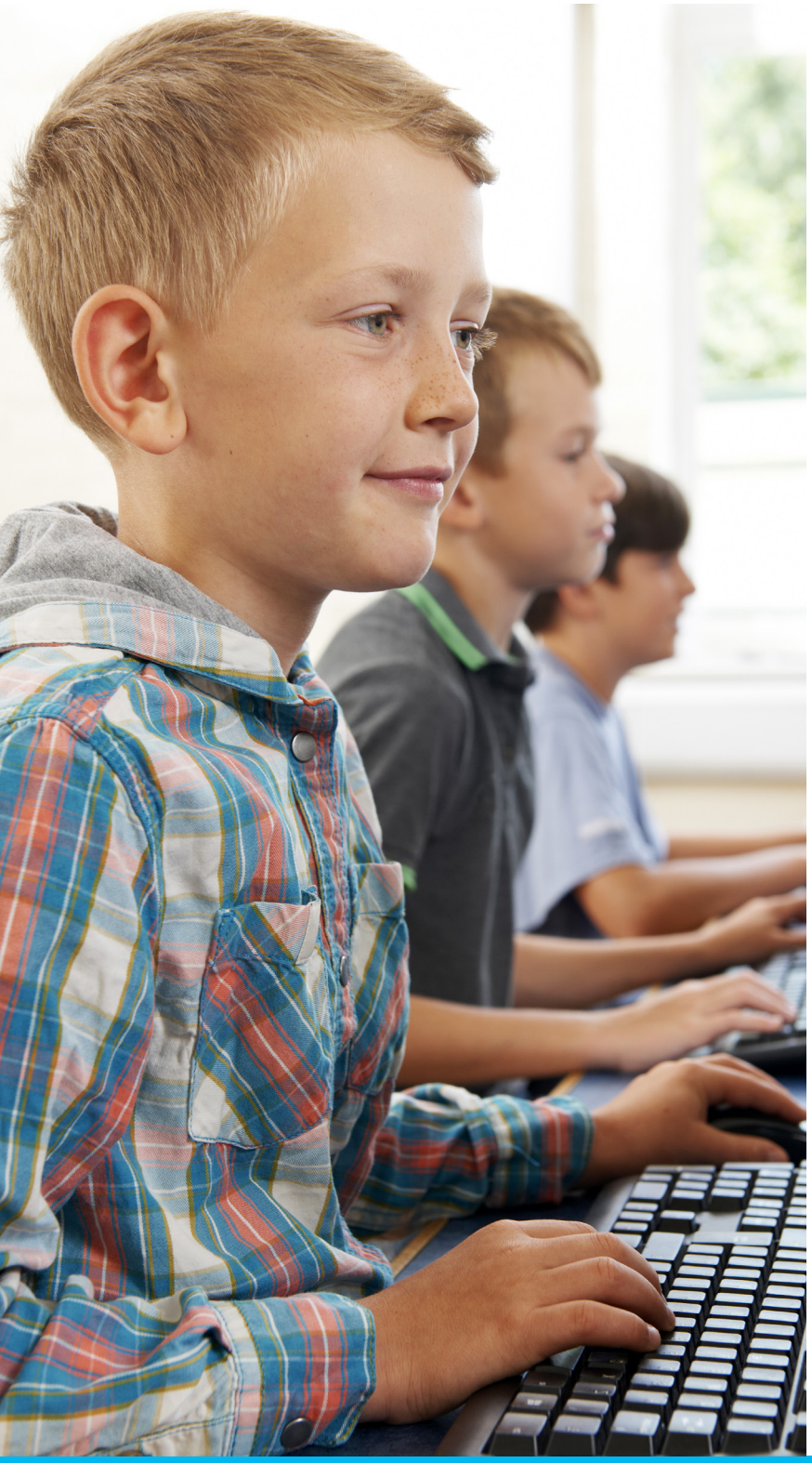
User security awareness

Humans are often the weakest link in the data security chain. While school districts may invest heavily in various tools and solutions to help protect student data, the human element plays a very vital role.

School districts should provide periodic security awareness to their staff and students, and continually reinforce the need to ensure data is kept private and secure. Awareness trainings should include modules that cover password security, email security, social engineering, and anti-phishing awareness. There are many providers of high quality and affordable security awareness training—one of the most cost-effective cyber security investments you can make.

Why Student Data Collection Matters

K-12 education technology companies are custodians—storing and taking care of crucial student data in products like student information systems (SIS), learning management systems (LMS), online registration systems, and finance and HR systems.



A district's edtech vendor has to ensure that protecting students' information is their highest priority through: 1) technology safeguards, 2) strict best practices policies, and 3) dedicated, professional staff. A lack of any of these three critical elements is a significant disservice to customers and the student data they are entrusted to protect.

Education technology companies partnering with schools and districts to manage student data must be dedicated to being good custodians of this sensitive information. These companies should invest heavily in designing advanced, safe software systems with thorough safety protocols and procedures. And finally, leading edtech companies should have the vision to create a professional leadership position dedicated to strengthening the system's safety.

Questions to Ask a K-12 Education Technology Vendor:

1. What are **proof points** that you take **student data security seriously**?
2. Is a **security evaluation** performed to a **recognized international standard**?
3. Are systems **independently tested** for security vulnerabilities?
4. Has the organization taken the **Student Privacy Pledge**?
5. Does the organization have an **ISO 27001 certification**, and is it successfully renewed each year?
6. Does the organization complete **SOC 2® Type 2 examinations** on its controls relevant to security, availability, and confidentiality for multiple applications?

Tips for Choosing Secure K-12 Education Technology And Vendors

Partner with someone that proves they take data security seriously

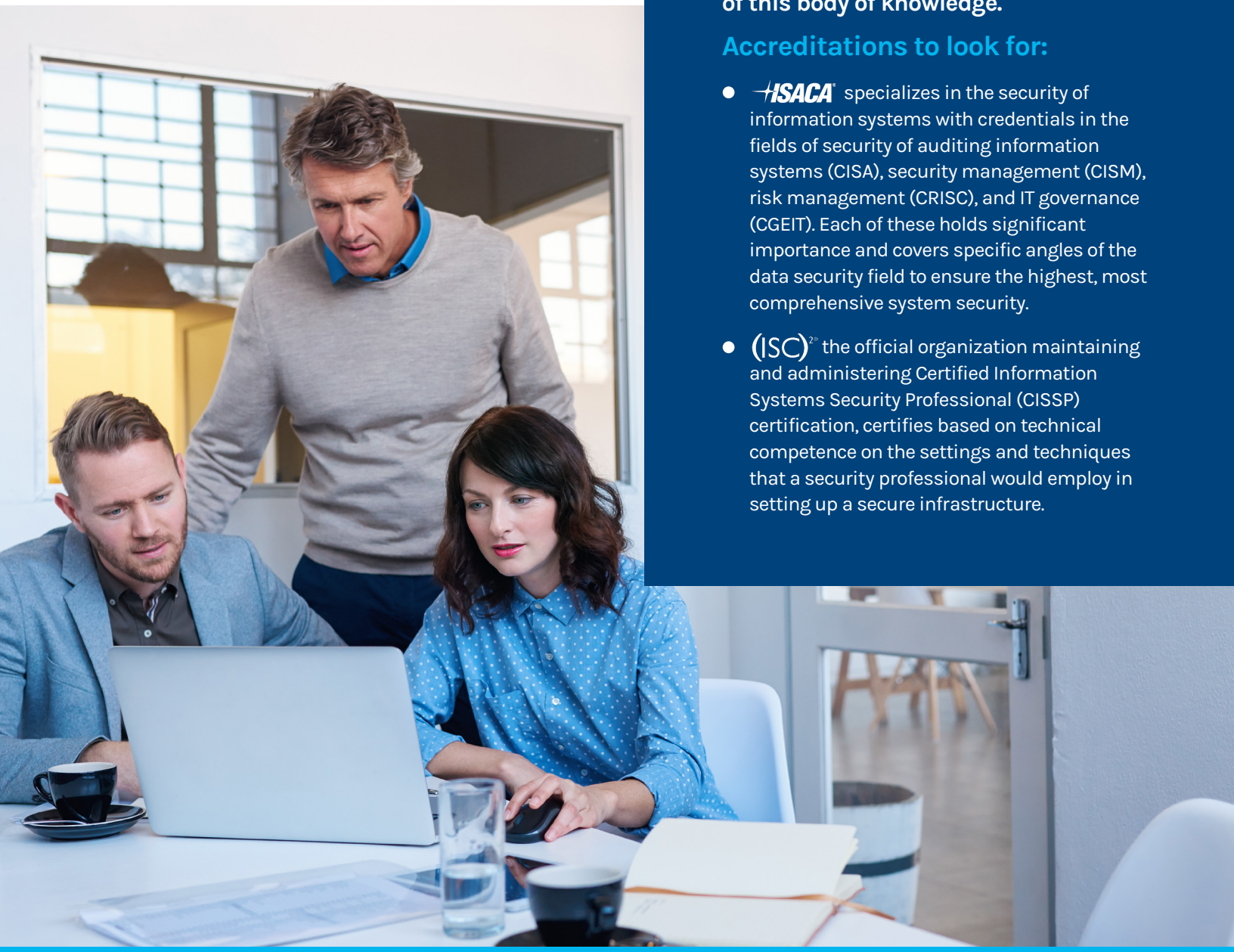
Student data security should be an edtech company's highest priority. Security can't be handled by a part-time position within the IT department. Schools and districts should partner with companies with an **experienced Chief Information Security Officer** with a proven track record of orienting the development and implementation of secure business software. This full-time role, reporting directly to the CEO and the company's Board of Directors, is responsible for defining the security posture and ensuring the design decisions to yield a secure, unified experience for customers.

A Chief Information Security Officer is ultimately responsible for ensuring that the company behaves as a good custodian of the data to which they have been entrusted. This is a role that requires extensive training, education, and experience.

Security professionals belong to a community with a common body of knowledge gained over many years, and there are a number of organizations that certify professionals in different aspects of this body of knowledge.

Accreditations to look for:

- ISACA® specializes in the security of information systems with credentials in the fields of security of auditing information systems (CISA), security management (CISM), risk management (CRISC), and IT governance (CGEIT). Each of these holds significant importance and covers specific angles of the data security field to ensure the highest, most comprehensive system security.
- (ISC)²® the official organization maintaining and administering Certified Information Systems Security Professional (CISSP) certification, certifies based on technical competence on the settings and techniques that a security professional would employ in setting up a secure infrastructure.



Look for "good custodians" of student data

K-12 edtech companies must take ownership and personal responsibility in securing student data. Good custodians are caretakers, rather than simply protectors. Caretakers fully understand the importance of caring for students' data and know how keeping it safe and impenetrable affects the well-being of students, families, and other stakeholders.

Good custodians of student data should make their commitment clear and visible by signing the Student Privacy Pledge, which safeguards student privacy regarding the collection, maintenance, and use of student personal information.

The Student Privacy Pledge states:

> "K-12 school service providers are honored to be entrusted by educators and families to support their educational needs and school operations. School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security."

Confirm best practices are in place & exercised

When a district or school partners with a student information system (SIS), parents and students should be invited into the secure system to enter their information. It's important that the company reviews all data and creates secure conventions for how the data is stored. Parents and students should know that their consent is required before any data is stored by the school or district.

When edtech companies adhere to best practices, schools and districts can assure stakeholders that sensitive information is safe. In turn, K-12 student data management vendors should provide schools and districts with clear, comprehensive best practices to follow.

Make sure the edtech provider can fulfill their obligations

Most obligations that education technology vendors meet in protecting personal data are common sense and common courtesy. However, courtesy—while common—is not universal, so there are some obligations that are enshrined in laws. The first is abiding by **FERPA, the Family Educational Rights and Privacy Act.** An educational agency or institution subject to FERPA can't disclose students' education records, or PII from education records, without a parent or eligible student's written consent. A student's health records maintained by an educational agency or institution subject to FERPA, as well as records maintained by a school nurse, are "education records" subject to FERPA."

Edtech companies must adhere to **Health Insurance Portability and Accountability Act (HIPAA).** The HIPAA Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

Ensure that only data that's useful/necessary is stored

Education technology companies should only store what they have a reasonable business need for. In aligning with a transparent communication model, companies need to ensure that the parent or guardian fully understands the purpose for which data is being stored. For example, an SIS should only store the minimum personal data needed to provide schools, teachers, parents, and students value from the product.

Many parents fear that their students' personal information will be sold to advertisers and they will be inundated with targeted marketing campaigns that they did not ask for. Vendors that store data have to take extraordinary measures to protect that data, and never sell personal data.

Confirm that basic protections are in place

1. **Data access should be provisioned on a strict business need-to-know basis.** Accountability begins by making sure that any access to data within the system is always under a unique username. For companies that host their customer's system, only employees with appropriate roles and who have passed background checks should have access to any systems on which customer data is present. It's also a good idea to publish similar guidelines for self-hosted customers in a security best practices guide.

2. **Keep unauthorized users out of the system (and network) where the data is stored.** A defense-in-depth approach should be used to ensure that only authorized people are on the network.

3. **Create whitelist capabilities** to limit access to the customer's system environment to ranges of specific IP addresses. Only requests originating from known locations should be given access to the system.

4. **Build intrusion detection systems** and check the network activity to ensure that it's consistent with student, teacher, and parent activity. If unusual activity is detected, procedures must be in place to set off a call tree and initiate countermeasures.

5. **Create least-privilege rules to ensure that authorized users only have access to authorized information.** Grant authorization based on job role, or more specifically, make sure people have only the authorization and access to the functionality and data needed to do their job and no more. The fewer people who have access to sensitive information, the easier it is to keep it secure.

Make certain that the system is resilient

When a school district entrusts its important student data to a software system, safeguards are necessary to ensure data will always be accessible even when inevitable disasters strike. In data storage and security, prepare not only for the improbable but sometimes the impossible. Data must be available when authorized users need it, which means school districts must be prepared for disasters and be able to quickly re-establish business processes if any interruption occurs.

Example—invest in providing warm backup facilities at geographically dispersed locations to ensure critical business systems will be back up and running in the case of any disaster.

Prove that the system is independently verified

Companies must independently verify the security management system. For example, as part of the independent assessment to the internationally recognized standard for Information Security Management Systems - ISO 27001, a SIS should undergo rigorous verification of its security system, including internal and external process verification. All external companies the SIS partners with should verify that its systems can withstand attack outside of this evaluation.

Confirm accountability for changes

Random or arbitrary changes made to a student's data can compromise data safety. An audit log of all changes to personal data should be written to ensure whoever makes a change can be held accountable for their changes.

Safeguard against data leaks through other systems

A good SIS or other data management system has interoperability with other software vendors, and best practices are to never send personal data to systems with lesser controls or controls that are untrusted.

A SIS needs to know where its sensitive data is. It should only offer data to other systems when those systems have verified capability to protect the data. Once they have verified their programs, the SIS should "sign" that program, and only programs that are exactly the same as when they were signed should be allowed to gain proper access to data in the system.

Trust edtech vendors with layered defenses

Good custodianship protects student data from being immediately compromised if a cyber threat occurs. Additional safety precautions must be in place to ensure that in the unlikely event someone breaks in, they cannot review any personal data or read files. Encryption is used to lock these files, and the key is hidden in the programs running the system. Look for vendors who perform annual third-party audits of their security management system.

Good custodianship protects student data from being immediately compromised if a cyber threat occurs.

Check that the vendor properly deletes outdated or unused student data

Trusted vendors don't keep data longer than it's needed for a defined business purpose. While data is in any form, it is vulnerable to misuse. An education technology vendor ensures that it only keeps data for which it has a defined purpose. Each type of record has a period of time during which it must be retained, and when it's no longer needed, it's deleted. Make sure a purge schedule is in place across all types of records, and records eligible for purge are removed quarterly.

Student data has to be thoroughly destroyed when it is no longer needed. When data is deleted, the data can no longer be recoverable by any means. Sometimes when the data can no longer be read by traditional programs, it can still be read by specialized tools, so it's imperative that data is securely destroyed and unreadable.

Good Custodianship Moving Forward

As more schools move to digital recordkeeping and the online classroom continues to grow, each student's educational experience will only be enhanced.

Personalized learning, increased collaboration, supported teachers, and better analytics must be matched with equally advanced safety precautions to ensure student information is secure.

Vendors of K-12 classroom management, student information systems, and other vital edtech products need to embrace the mantle of good custodianship and make data security their highest priority. Rather than make the news because of security breaches impacting students, education technology companies need to take charge and lead with advanced technology safeguards, best practices policies, and an investment in security professionals in leadership positions.

Companies taking personal responsibility through a commitment to these tenets are demonstrating a genuine custodianship of student data security to best serve students, parents, schools, and districts.

Sources

[1] **"Apple security flaw 'actively exploited' by hackers to fully control devices," The Guardian,** https://www.theguardian.com/technology/2022/aug/18/apple-security-flaw-hack-iphone-ipad-macs**. Aug. 18, 2022.**

[2] "Massive data leak exposes 700 million LinkedIn users' information," Fortune, https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/. June 30, 2021.

[3] "533 million Facebook users' phone numbers and personal data have been leaked online," Business Insider, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4. April 3, 2021.

[4] "Growing Frequency and Rising Costs of Ransomware Attacks on Schools Highlight New Report," THE Journal, https://thejournal.com/articles/2022/03/10/growing-frequency-and-costs-of-ransomware-attacks-on-schools-highlight-new-report.aspx. March 10. 2022.

[5] "FBI Flash: Increase in PYSA Ransomware Targeting Education Institutions | CISA." Cybersecurity & Infrastructure Security Agency, www.cisa.gov/stopransomware/fbi-flash-increase-pysa-ransomware-targeting-education-institutions. Accessed Aug. 18, 2022.

[6] Bischoff, Paul. "Ransomware Attacks on US Schools and Colleges Cost $3.56bn in 2021." Comparitech, www.comparitech.com/blog/information-security/school-ransomware-attacks, June 23, 2022.

[7] 2022 Data Breach Investigations Report. Verizon Wireless, https://www.verizon.com/business/resources/reports/dbir/. 2022.

[8] "Hear Ransomware Victims Describe the Response & Recovery Lessons Learned at Virtual Event for IT Practitioners," THE Journal, https://thejournal.com/articles/2022/08/03/it-practitioners-invited-to-hear-ransomware-victims-describe-lessons-learned-in-aug-16-webinar.aspx?s=the_nu_040822&oly_enc_id=6722E9655690A3A. Aug. 3, 2022.

[9] "Teens, Social Media & Technology 2022," Pew Research Center Report. https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/.

[10] "80% of American Parents Worry About Children's Online Privacy, but Only 48% Monitor Activity Regularly." Pixalate, www.pixalate.com/blog/childrens-online-privacy-harris-poll-coppa. March 2, 2022.

[11] "Probable security breach may have compromised thousands of Lewis Palmer students' data." The Complete Colorado Original Reporting & Commentary. http://completecolorado.com/pagetwo/2016/05/24/probable-security-breach-may-have-compromised-thousands-of-lewis-palmer-students-data/. May 24, 2016.

PowerSchool

Powering Brighter Futures

For more information on K-12 student and school district data security, visit:

https://www.powerschool.com/security/

WP_SISTL-878373_090222