DATA SECURITY & PRIVACY:

A BLUEPRINT FOR ALL SCHOOL DISTRICT LEADERS

IN COLLABORATION WITH
The RTM National
K-12 Advisory Board

2018

RTM BLUEPRINT

If you would like to take part in future Blueprints or learn more about the work RTM is doing with school districts, please contact

info@rtmbusinessgroup.com

Authors

Sheryl Abshire, Ph.D.
Chief Technology Officer
Calcasieu Parish Public Schools (LA)

Joseph Williams
Executive Director of Technology
Perris Union High School District (CA)

Jeff McCoy
Associate Superintendent of Academics
Greenville County Schools (SC)

Scott Bailey
Superintendent
Desert Sands Unified School District (CA)

Table of Contents:

Key Questions to Consider

- How important is protecting the privacy of student data?
- What key steps do district leaders need to take in order to ensure student data privacy?
- How do we communicate to parents and community stakeholders the policies and procedures that keep their students safe while online?

62% 62% of education IT leaders said concerns around privacy and security are more important than they were last year, with 30% saying it was "much more important."[1]

60% SSO is the most-implemented interoperability initiative, with 60% of school technology leaders having partially or fully implemented SSO.[1]

60% Data interoperability was the next most popular solution, with 73% of respondents indicating they were in planning or implementation stages.

3rd Among education IT leaders, cyber security is now ranked as the third highest priority and privacy is fourth, up from 2014 where privacy was ranked second to last.[1]

90% 90% of respondents expect their instructional materials to be at least 50% digital within the next three years.[2]

87% 87% of individuals are concerned their data is shared without their knowledge/ consent.[3]

66% 66% of Americans would accept less personalized content/fewer discounts to keep their personal information private.[3]

Introduction - Call to Action

A critical emerging issue that confronts district leaders across the country is student data security/privacy. It is important to create a collaborative culture that welcomes ongoing conversations about data security and privacy across all departments in the district office in order to continuously improve processes and practices. School district leaders should be engaged in constantly defining and redefining priorities, processes and procedures in their districts around student data security and privacy.

Districts must remain vigilant when it comes to keeping their students safe. Today, that involves much more than physical safety. The digital environment holds many potential dangers and leaders must understand these threats in order to keep students safe in a digital environment. This blueprint will assist district leaders as they create processes, procedures and structures to assure their district not only meets strict compliance with state and federal mandates, but assures communities, that at all times, data privacy remains a top priority.

Data Governance and Stewardship

Data governance is an organizational approach to data and information management that includes policies, procedures, and standards regarding data security and privacy protection, data access, and data sharing. A comprehensive data governance program helps to ensure that data management and protection procedures are in place to reduce data privacy and security risks due to unauthorized access or misuse of data.

One of the first steps in assessing and improving a district's data security environment is the establishment of a Data Governance Committee/Team. It is imperative that districts establish this committee in order to properly assess and plan the important work of collecting, archiving and protecting (securing) the district's data assets.

Some members of the Data Governance Committee could include participants from the following departments/groups:

- Auditing/Risk Management
- Pupil Services
- Information Technology
- Student Information Systems
- Curriculum, Instruction and Assessment (Academics)
- Special Education
- Finance/Purchasing
- Personnel/Human Resources
- Principal Representation
- Teacher Representation

In some districts, particularly smaller ones, it may not be clear as to what needs to be done to effectively protect student and district data. Assumptions will be made and the risk for a breach is higher. The ideal checklist for a cyber security strategy includes several components, the main being instilling better behaviors. In order to protect student data, everyone outside of the IT department needs to accept their role in cyber security. Clarifying the language used with non-IT personnel will help them in achieving these strategic goals.

As an example, the data governance committee might be tasked with approving the purchase of new technical and digital resources, as well as changes to any existing technical and digital resources. The data governance committee provides training and direction to data stewards responsible for specific technical and digital resources. A formal campaign to engage and inform the board and all stakeholders of the procedures and policies is a best practice.

Data security is an issue of continuing concern to K-12 districts. Role-based security is a process that is critical in determining what data is available, and to whom and when this data is available. The use of role-based security can significantly reduce risk when properly implemented. The level of access each employee and/or contracted service provider receives should be standardized and customized based on their current role in the district or their need to access certain data points. As an example, a special education supervisor/coordinator working with a specific grade in one school should not automatically gain access to students at other schools. Access to data should be granted based on what is needed by the staff member to effectively do their job. Districts should consider adding clauses about data privacy in their AUP or in a Data Confidentiality Agreement.

Having the ability to track who accesses what data is critical in order to protect student privacy and reduce liability. Systems that monitor and record staff access to student records and monitor content on various data stores can protect the district in cases of lawsuits. In addition, a single sign-on system ensures proper access to district systems in a standardized way.

Security Audit and Threat Assessment

Security audits and threat assessments are important to ensure the district is doing everything possible to protect student data. A security audit can take different forms, but typically involves a measurable technical assessment of district systems and potential risks to data breaches. A first step might be to accurately inventory the digital asset, systems and processes used in the district and in classrooms in order to determine exactly what data is being collected.

School districts can mitigate the threat of a data breach. By conducting a self-assessment of risk, The self-assessment is designed to assess the effectiveness of privacy and security controls with a focus on identifying practices and procedures that improve the security of student, staff, and parent/guardian information. In the wake of data privacy concerns, companies have evolved that offer self-assessment services if a district wants to contract with a third-party. Categories for self-assessment may include user accounts, response plan, security controls, user awareness training, and business partner accountability plans.

- User accounts must be proactively monitored. Periodic reviews of user access to data can ensure that access remains appropriately aligned with employee role and function. Policies and procedures should include the ability to immediately terminate user access following employee termination or voluntary separation.

- Districts may also consider the development of response plans that protect data in the event of a breach. Districts should consider exercising the plan just as they would other emergency response plans.

- Security controls may include assigning responsibility for creating, implementing, and maintaining security policies and procedures. Such policies and procedures may include a requirement to periodically change passwords.

- As the implementation of more robust information systems have become more reliant on electronic data, proactive user awareness programs become paramount. Without adequate training, users present a constant threat to the integrity of the system.

- Districts must be mindful of business partner contracts. Processes should be developed to ensure software acquired from business partners complies with data security principles. Third-party relationships, data privacy assurances, and data destruction guidelines should be adequately addressed in agreements.

Data Breach and Identity Management Protocols

A data breach is generally defined as an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information maintained by the entity. Personally Identifiable Information (PII) may include individuals' names or initials, social security numbers, driver license number or identification numbers, financial information, medical information, and/or health insurance information. Districts should check their state laws as each state defines PII differently. School districts should create data breach response protocols/plans to guide them before, during and after a data breach.

Identity management refers to an integrated system of business processes, policies and technologies that enables organizations to facilitate and control user access to critical online applications and resources while protecting confidential personal and business information from unauthorized users.

Post-breach protocols may include:

- Identifying the type of data that was breached and how the breach occurred.
- Taking steps to prevent further data breach or loss.
- Conducting interviews of the parties involved.
- Securing backups on systems or platforms that store data.
- Determining if the data breach was related to password and/or encryption being compromised.
- Determining the need to change passwords, credentials, or profiles and revise security measures.
- Identifying decision-making authority and employee expectations.
- Crafting a public response plan or letter.
- Determining the district's legal responsibilities.
- Notifying the people that were impacted by the breach. Law enforcement and state law may influence the notice.
- Notifying employees that may have been logged into the system when the breach occurred with recommendation to change passwords and security information.
- Determining what training (or retraining) needs to take place to prevent future breaches.

(For a more detailed example see **Data Breach Response Checklist | (https://bit.ly/2qY27b9)**

Partnerships and Alliances

Scrutinizing solution partner agreements is important, even if it delays using the educational tool that is being purchased through that agreement. Purchase orders should not be approved until the school district has agreed upon the data privacy clauses concerning student data. Adding a Student Data Security and Privacy addendum to your agreement with your existing partners ensures that you have taken the appropriate actions, if the original contract does not meet the district's data privacy standards and state and federal requirements. You should consult with district legal counsel to ensure the addendum meets your legal needs.

Know that it is not a matter of **IF**, but a matter of **WHEN** a data breach will occur. Districts need to be covered by the fact that they have a signed data privacy document from their solution partners, stating clearly that they understand and agree to comply with designated guidelines so that they can be held accountable when something does happen. In many districts, sensitive, protected data sits across many systems, and this data is potentially at a greater risk for exposure.

Some large solution partners are ISO27001 certified (https://goo.gl/sbJUre), which in some school districts or states becomes an allowable exclusion to signing the district's data privacy security agreement and addendums. This certification demonstrates that these solution partners have proven to comply with the standards set by the International Standards Organization in 2014 for protecting PII.

Before the days of storing data on cloud resources, tracking a data breach and identifying its cause was much simpler. With the advent of cloud storage, this can be much more complex. Data sharing agreements with partners should contain such things as where they store and host district data. It is important to determine if any cloud data is hosted on servers in other countries. Once the data leaves the borders of the United States, it can be difficult to investigate and hold people accountable. How data is destroyed once contracts are ended is another clause that should be contained within data sharing agreements. Any change vendors make to how data is handled should be reviewed by both parties and new data sharing agreements should be signed to cover any new changes.

Parents should be aware of how student data is being shared. There must be a communication plan for letting parents know how data is being collected and used. A student data security privacy agreement should indicate how parents, legal guardians and eligible students can review any and all

of their student's data, including data held by third-party solution providers. Additionally, the solution provider and the district need to have procedures in place for notifying the district and affected parents, legal guardians or eligible students when there is an unauthorized disclosure of data.

Compliance with federal and state law is imperative, but you can take additional steps with the partner to ensure data is protected. Periodically, revisit processes and procedures internally and with your solution providers to make sure there have been no modifications. A thorough investigation of business partners' usage of data for advertising purposes must be conducted. Risk managers and high level administrative staff can possibly mitigate future problems by adding cyber liability insurance onto their existing physical property insurance policy to address the aftermath of future breaches.

Data security must be a non-negotiable in order to ensure compliance. For example, some districts may be willing to modify clauses on a case-by-case basis, for instance, to accommodate anonymized data being used for research purposes for up to a year beyond the contract termination date. Data retention or data destruction past the termination of an agreement is a common source of disagreement that can delay purchasing and implementation. Data sharing agreements should list actions that the solution provider must take with student data and PII after the termination, cancellation, or expiration of the contract.

Schools, districts, states, and other entities may want to form a "Student Privacy Alliance" to aid in the legal requirements, contracts, and to manage the resources needed for student data privacy and security. Two examples of alliances are the Massachusetts Student Privacy Alliance (MSPA) (https://goo.gl/H8tJoQ) and the California Student Privacy Alliance (CSPA) (https://goo.gl/MdVbkY). These organizations establish a collaborative community to share effective practices, provide tools and resources for data governance, create common solution partner applications, develop standardized privacy agreements, provide searchable databases, and maintain inventories of digital resources.

Compliance and Risk Management

In order to comply with state and federal laws, district leaders must consider the key steps needed to ensure student data privacy. It is critical to assure that parents and community stakeholders understand and support district efforts to protect students online. Proactively creating policies and procedures will assure the district is thoughtfully reacting to data concerns. It is critical that those responsible for data privacy and security know both the constantly changing state and federal laws that govern privacy and security in their state. Leaders must be aware of changes in order to meet compliance standards, as well as helping others digest this information. According to the Data Quality Campaign, in 2017, 36 states introduced 95 bills and passed 31 new laws addressing the collection, linking, and governance of education data. Additionally, in 2017 legislators in 42 states

introduced 183 bills and passed 53 new laws in total that explicitly address how the state collects, manages, uses, reports, and protects data about students and schools.

The introduction of prior legislation, such as the Student Digital Privacy and Parental Rights Act[4] of 2015 and the Student Privacy Protection Act[5], and the Safe Kids Act[6] are indicative of a national and congressional mood to further legislate the use of student data in schools.

In California, the Student Online Personal Information Protection Act (SOPIPA)[7], was put in place to keep large companies from using analytics on student data to build profiles for targeted advertising. SOPIPA prevents tech companies from using and selling student data for profit. It also requires companies to better safeguard the data and delete certain information upon request from a school or parent. Many states have used the guidelines in SOPIPA to develop particular state policies regarding data security and privacy.

In short form, these are the major federal laws you should know:

HIPAA: Health Insurance Portability and Accountability Act

Protects a student's identifiable health records (or any health-related condition or information, in any medium or form) from being disclosed to anyone outside of the school, except other healthcare professionals directly responsible for caring for that child.

FERPA: Family Educational Rights and Privacy Act

https://goo.gl/TFvxzr

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

COPPA: Children's Online Privacy Protection Act

https://goo.gl/sezWuY

COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

CIPA: Children's Internet Protection Act

https://goo.gl/5Apr5h

Requires schools and libraries receiving E-rate funds to "block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors)."

PPRA: Protection of Pupil Rights Amendment

https://goo.gl/kzrxPH

The Protection of Pupil Rights Amendment (PPRA) is a federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature. PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors.

Some programs are emerging to help districts, staff, students, and parents attain digital literacy and digital citizenship. CoSN and Common Sense Media are two examples of organizations with these resources. Getting a certification from CoSN's Trusted Learning Environment (TLE) Seal Program (http://trustedlearning.org/about-the-seal/) helps instill trust from the community. The TLE Seal is a mark of distinction for school systems, signaling that they have taken measurable steps to implement practices to help insure the privacy of student data. By obtaining the TLE certification, districts review and analyze their processes in five areas of practice to ensure that adequate steps are being taken to secure district data. CoSN has developed the TLE Seal in conjunction with the School Superintendents Association (AASA), the Association of School Business Officials International (ASBO International), and the Association for Supervision and Curriculum Development (ASCD).

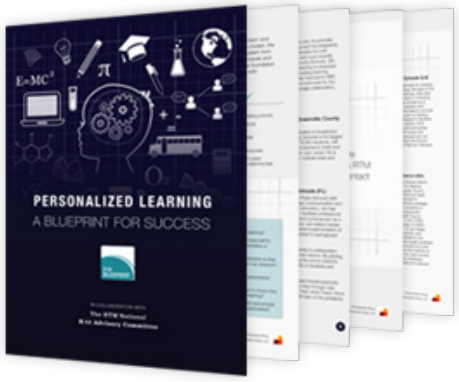
Likewise, Common Sense Media provide teachers, parents, students, and policymakers with tools and resources for digital literacy and digital citizenship. Some of these tools include K–12 Digital Citizenship Curriculum, ratings and reviews of apps, websites, games, etc, and resources for advocacy. Common Sense Media has certifications for districts, teachers, and students. When a district takes the time to obtain this certification, it shows they have taken measures to keep students safe while using technology in the classroom.
(https://www.commonsense.org/education/certification)

Data Security's Impact on Teaching and Learning

Data security has a significant impact on teaching and learning in the classroom. It is imperative that teachers understand the laws governing student data security and privacy since they are the "primary guardians" of student data.

In technology-rich environments such as personalized and blended learning, it is critical that school employees are keenly aware of the district policies and procedures surrounding data security. For districts that have already embarked on a personalized and/or blended learning journey, it is never too late to review and/or establish stronger data security policies. Personalized learning is an innovative approach to advancing student learning. However, it can also create vulnerabilities in a district's data security plan. It is critical that districts conduct extensive planning when embarking

on a journey to personalized learning. A resource that may help districts implement personalized learning can be found at http://www.k12innovationforum.com/rtm-blueprint.



Districts should consider creating a checklist of data security precautions prior to beginning a personalized learning and/or blended learning project. Many districts have already implemented these innovative learning environments and have created processes to guide the use of data. Collaborating and consulting with these districts may provide insight on best practices.

Some districts depend on and use legacy programs. These programs may have unknown gaps in security and/or compliance. With these legacy programs, it is recommended that your district work with the provider to transfer the data in compliance with current laws. In turn, the district should outline guidelines/ timelines for the legacy programs to bring them into compliance.

In today's digital environment, many state standards contain indicators for accessing content and using programs online. In order to meet these standards, teachers are required to transform their teaching and learning environments. While some teachers may see data security policies and practices as intrusive or anti-innovation, innovating "within the box" is still possible. Be cognizant that innovation does not imply just purchasing more technology. You can innovate while working within the compliance framework that the law requires, to George Couros' point in The Innovator's Mindset. (https://goo.gl/Ck9ypm)

Protecting students online must be one of the top priorities for educators and parents. Parents must understand the district's data security and privacy procedures in order to feel comfortable with giving students permission to access district technology resources. In today's environment, it is difficult to educate students effectively if they do not have permission to access digital resources. Data security policies do not have to stifle innovation or the use of technology. They do require that teachers plan ahead so that any tools or applications they want to use in the classroom can be vetted through the policies and procedures established by the Data Governance Committee.

Data governance policies should give educators the framework, processes and procedures to obtain the tools they need to effectively educate students while at the same time keeping student data safe. Administrators can foster innovation by creating learning environments where teachers know innovation is encouraged. However, it is essential they clearly understand, they may have to amend their practices in order to be compliant with data security policies. Teachers need to know they might have to anonymize student data if they are using free resource or software.

Striking the right balance so that educators do not feel they work in a climate of fear and distrust is essential to creating an innovative and effective learning environment. Educators must feel confident they have the assistance to use tech tools appropriately. They should be empowered to use resources they feel are appropriate in improving teaching and learning. However, teachers must have the background and professional learning that allows them to help students use technology resources effectively and safely.

Innovation and keeping students safe are not mutually exclusive. There needs to be an awareness district-wide that student safety does not need to hinder innovation. The debate does not have to be two-sided. There is nuance to this debate: a sliding scale depending on district size, administrative structure and state law is ideal.

Parental and Community Engagement

In today's world of data visibility, parents are often times concerned about their child's privacy online. It is critical to engage parents and community in the conversation surrounding data privacy and security. School districts can use a variety of methods to communicate information to parents around data privacy. Many districts provide training to parents surrounding the issues of data security. These trainings often include helpful tips on how to keep students safe while they are at home and at school. School districts may be able to partner with local law enforcement offices to offer cyber safety trainings to parents. Keeping students safe online is the responsibility of the entire community.

The majority of parents do not know how their schools collect, use, store and destroy student data. At a national level, surveys (conducted by the Future of Privacy Forum) have shown that informed parents support the use of student information if it helps with student learning goals. In today's educational landscape, it is imperative that we prepare students for the global world they will live in. This often requires them to use online tools to collaborate, share information and research. These critical soft skills are important for their future success in college and careers. Parents can be strong advocates if properly engaged and informed.

Educating District Staff Through Professional Learning

Educating your staff about data breaches and security protocols is critical in order to effectively prevent potential threats to student privacy. All staff, including classified and non-classified staff should understand what data breaches are and the steps needed to contain them. Training programs should be developed and required of all staff based on their jobs and access to data. Additional training may be required for staff who violate the security protocols outlined by the district.

Educators live in a world of apps, online programs and online tools that appear instructionally focused. However, in many cases, these apps and tools have hidden threats when it comes to student privacy. It is critical that district office staff communicate the importance of processes, protocols and standards when it comes to using various systems, apps and programs in the classroom. Teachers and administrators must be made aware of the district process for requesting access to system, apps or programs they want to use in the classroom so that student data can be protected.

Ongoing and consistent training is key to ensuring a culture of vigilance when it comes to data privacy and security. Periodic training on data security and privacy is necessary, but “ongoing” reminders need to be integrated into other types of workshops so that staff and teachers are reminded of the importance of data security throughout the year. All professional learning needs to utilize simple language, not technical terms, in order for it to be effective. Some districts incorporate their policies and procedures into beginning of the year videos that all staff are required to watch so that a consistent message is being sent to all staff.

Teachers are the first line of defense when it comes to protecting student data. Personnel with access to the Student Information System (SIS) or anyone with access to more critical data, such as student health, grades, attendance, and social security numbers, require more intense training. A major component of the “how to use the system” training must be a focus on the data privacy aspect. In some districts, users with access to data systems (including teachers) are required to sign a special Data Confidentiality Agreement. This agreement usually contains language about keeping student data safe and the consequences for violating the agreement.

In order to create a culture of vigilance around data security and privacy, districts must have a clear plan to regularly monitor and enforce practices and policies. The state of Missouri, for example, has a Cyber Aware School Audits Initiative (https://goo.gl/onVEr8), that measures the need to protect the student PII collected at the district level.

Closing

Data privacy and security is everybody's responsibility in a district. As a school district leader, it is essential to lead by example. From the simple task of logging off a computer when leaving a desk, to never loading sensitive data on an external storage device, everyone is responsible for the safety and security of the district's data. Whenever possible, aggregated, de-identified data that do not identify individual students should be used to inform key policy decisions and help improve services and systems that benefit students. This blueprint, while not a comprehensive, single solution for a district to follow, is a guide that will help stimulate thinking and planning for districts seeking to assure that they are following data security best practices.

Resources:

- Data Privacy Guidebook (https://www.f3law.com/privacy)
- PUHSD Data Security and Privacy Agreement (https://goo.gl/42P2UW)
- Center for Digital Education (https://goo.gl/DyWRua)
- Data Quality Campaign (http://dataqualitycampaign.org)
- Student Data Principles (http://studentdataprinciples.org)
- Trusted Learning Environment certification: (http://trustedlearning.org)
- FERPA/Sherpa (https://ferpasherpa.org)
- CoSN's Protecting Privacy in Connected Learning (www.cosn.org/privacy)
- CoSN's Cyber Security for the Digital District (http://www.cosn.org/cybersecurity)
- CoSN & DQC Collaborative Effort (https://goo.gl/9mhD25)
- Data Quality Campaign (www.dataqualitycampaign.org)
- Student Privacy Pledge (http://studentprivacypledge.org)
- USDE Privacy Technical Assistance Center (https://studentprivacy.ed.gov/)
- Making Sense of Student Data Privacy (http://www.k12blueprint.com/privacy)
- National Cyber Security Alliance (www.staysafeonline.org)
- Protecting Student Data Training Video (USDoE) (https://goo.gl/1GJfvj)
- Common Sense Media (http://www.graphite.org)
- Trends in Student Data Privacy Bills in 2016 (https://goo.gl/VKz43W)
- California Student Privacy Alliance (https://goo.gl/MdVbkY)
- Massachusetts Student Privacy Alliance (https://goo.gl/H8tJoQ)
- California AB 1584 Compliance Checklist (https://goo.gl/kdvVGw)
- PTAC Data Breach Response Checklist (https://bit.ly/2qY27b9)
- Google ISO 27001 Certification (https://goo.gl/KshXe3)
- Microsoft ISO Certification (https://goo.gl/8yoZ1b)

1. CoSN 2017 IT Leadership Survey - http://www.cosn.org/sites/default/files/CoSN_ITLdrship_Report_2017_040317.pdf
2. CoSN 2016 IT Leadership Survey - https://thejournal.com/articles/2016/05/24/it-leaders-see-broadband-and-network-capacity-as-top-priorities.aspx
3. National Cyber Security Alliance
4. https://www.congress.gov/bill/114th-congress/house-bill/2092%09
5. https://www.congress.gov/bill/114th-congress/house-bill/3157
6. https://www.congress.gov/bill/114th-congress/senate-bill/1788/text
7. https://termsfeed.com/blog/sopipa/