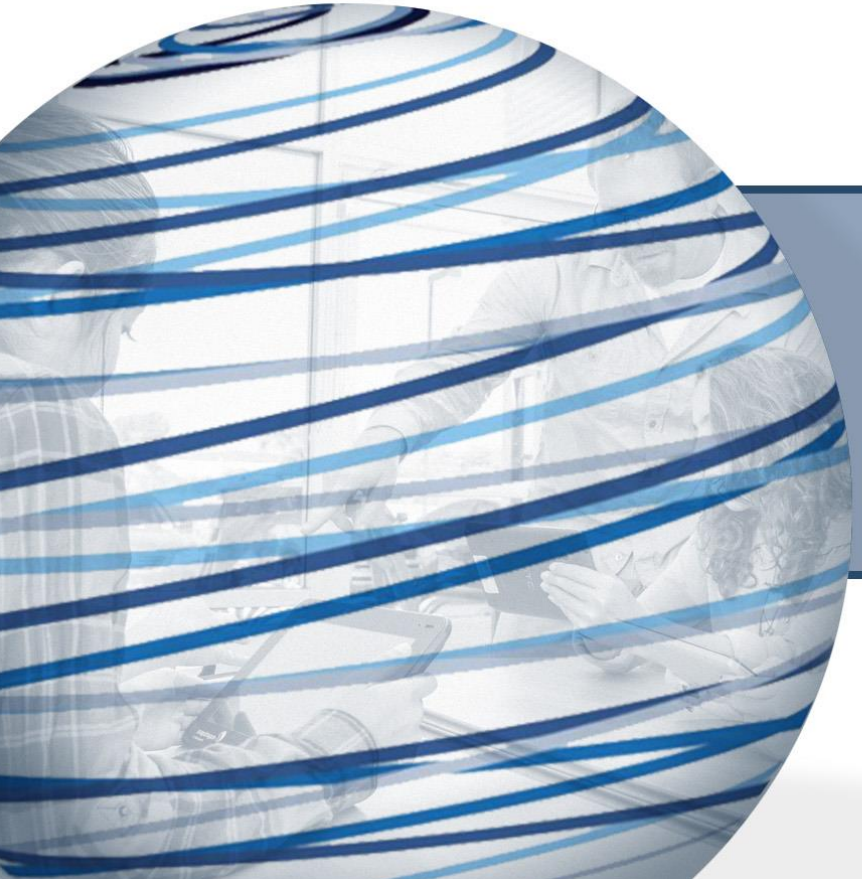


LEADING EDUCATION INNOVATION

Student Data Privacy and Distance Learning During CoVID

Linnette Attai

Project Director, CoSN Privacy Initiative and
Trusted Learning Environment Program

LAttai@cosn.org

About CoSN

Transforming Education Through Visionary Technology Leadership

Premier professional association for K-12 school system education and technology leaders

- Providing management, community building, and advocacy tools you need to succeed
- Representing over 13 million students in school districts nationwide
- Empowering educational leaders to create and grow engaging learning environments

Introductions

Linnette Attai
Project Director,
CoSN Privacy Initiative and Trusted Learning Environment Program
Lattai@cosn.org

Linnette Attai is Project Director for CoSN's Privacy Initiative and Trusted Learning Environment Program. As founder of the global compliance consulting firm PlayWell, LLC, Linnette delivers strategic advice and training, policy development, and technology assessments, and builds cultures of compliance across a wide range of organizations. She also serves as virtual chief privacy officer and GDPR data protection officer to select clients.

Linnette is a recognized expert in the youth and education sectors and speaks nationally on data privacy matters. She is a TEDx speaker, advisory board member for the Ithaca College Cybersecurity Program, and author of the books, "Student Data Privacy: Building a School Compliance Program," "Protecting Student Data Privacy: Classroom Fundamentals" and "Student Data Privacy: Managing Vendor Relationships."

Introductions

Jennifer Miller
Director, Cybersecurity, Acquisitions, and Performance Excellence
Cypress-Fairbanks ISD

TLE Seal Recipient
Since 2019

Jennifer is the Director of Acquisitions and Customer Support in Cypress-Fairbanks ISD. In this dual role, working for the 3rd largest district in the state and the 23rd in the country, Jennifer is responsible for the Customer Care Center and the Acquisitions Teams that serve over 14,000 employees and 115,000 students. In this capacity she provides leadership for the Customer Care Center staff and district's Acquisitions team. The Acquisitions Team purchases all of the software and hardware for the district. This year, the Customer Care Center team has already answered over 27,000 phone calls for support from staff, students, and parents. She is most proud of developing a performance excellence program that has resulted in: 92% customer satisfaction, meeting target resolutions for our stringent service level agreement, and developing key performance indicators for the department.

Jennifer is in her 30th year in Cypress-Fairbanks ISD. Jennifer began as a classroom teacher, teaching fourth grade for 4 years and first grade for 1 year prior to beginning her service in the Technology Department. Jennifer initially served as the Technology Training Coordinator in the department and then served as the Help Desk Manager before serving in her current role. Jennifer loves seeing the great strides the district has made in providing current technology devices and connectivity in all classrooms.

Jennifer serves on the Consortium of School Networking (CoSN) Governance Committee at the national level, working with national education technology leaders in K-12 on developing rigorous standards for developing Certified Education Technology Leaders (CETLs). Jennifer also serves on the Board of the Texas K12 CTO Council as the Board Secretary. She thoroughly enjoys helping teachers and students learn and utilize technology in new and exciting ways.

Introductions

Derrick Johnson,
CISSP, CISA, CISM
Director, Information Technology Security
Fulton County School System

TLE Seal Recipient
Since 2016

Derrick Johnson has more than 30 years in Information Technology. He is currently the Director of Information Technology Security for the Fulton County School District, Atlanta GA. In his current position, he is responsible for Technology Security & Data Privacy operations that serves over 95,000 students and 14,000 staff.

Throughout his career Mr. Johnson has advanced in the information technology industry by staying current and passionate to the profession. His vast knowledge and professionalism have enabled him to strategically develop and manage various security and network operations from small to large scale enterprises.
He began his career as a Field Service Engineer & Technology Instructor, with Digital Equipment Corporation. At Digital, he taught client server system management support courses to Digital's internal support personnel and customers across the US. His career has expanded with numerous IT Network & Security support and management positions in Corporate, State and Local government in the information technology arena.

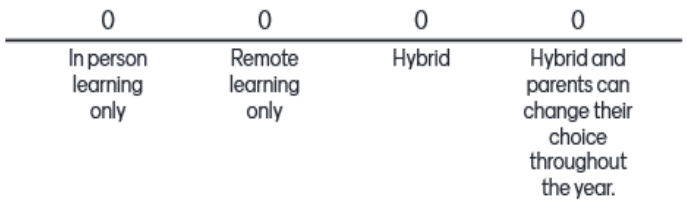
Derrick holds numerous IT certifications including but not limited to ISC2 CISSP, ISACA CISA and CISM and Cisco's CCNP. Mr. Johnson is a graduate of Atlanta Technical College with a major in Computer Technology.

.

Go to **www.menti.com** and use the code **72 77 08 3**

Mentimeter

Is your district currently...



Go to **www.menti.com** and use the code **72 77 08 3**

What are your most pressing privacy concerns in remote or hybrid learning environments?

Mentimeter


Time for change

No Shortage of Privacy Concerns

- Videoconferencing
- Training
- Device distribution
- Classroom software
- Network security
- Ransomware
- Health screenings…

…and no roadmap to follow

CoSN's Trusted Learning Environment Seal Program is a privacy framework customized for the needs of school systems.

Managing Privacy in a Crisis

- Privacy matters, now more than ever…
- Rely on your foundation.
- If you haven’t built a foundation, begin the journey with a few simple steps and keep to the plan.

Critical Leadership Needs

- Understanding plus active discussion and deliberation related to data privacy and security
- Up to date policies and regulations addressing data privacy compliance requirements.
- Clear policy expectations for the protection of student data privacy and security, as well as the transparent use of data
- Adequate resources to meet data privacy and security needs.

CoSN's Trusted Learning Environment Leadership Practices

Train, Educate, Rinse, Repeat

- **Train** on data privacy regulation, district policy requirements and procedures
- **Educate** parents and students and provide resources on data privacy, security and media literacy
- **Audit** policy and procedure compliance

Additional Resources:
10 Steps Every District Should Take

Who Needs to be Involved?

Privacy involves everyone in the district.
Everyone who touches student data is responsible for behaving in ways that protects the information.

A privacy leader is needed,
but the work is everyone's job.

Get Down to Fundamentals

Protecting student data is a team effort

- **Leadership emphasis** on the importance of the privacy work, prioritizing privacy with technology providers and requiring active participation across teams
- **Engage** multiple stakeholders to effect change across teams
- **Identify**, **develop** and **adopt** necessary policies and procedures

What Does it Take?

If we change our behavior, we reduce our risk.

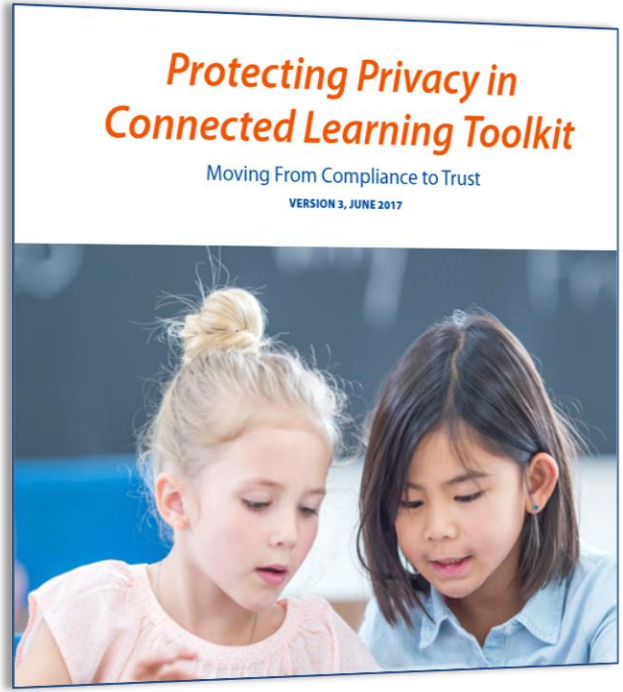
Be proactive.

Where to Begin?

Refresh on the Fundamentals

FERPA, PPRA, COPPA and more…

Privacy: *Making the Case to Leadership*



CoSN
LEADING EDUCATION INNOVATION

Build Your Foundation

Behavior, guided by policy, backed by procedure.

PROTECTING PRIVACY IN CONNECTED LEARNING INITIATIVE

Trusted Learning From the Ground Up: Fundamental Data Governance Policies and Procedures

NOVEMBER 2019

Training		
Policy requiring periodic privacy and security training for staff with have access to education records	Process for maintaining record of training	*Example Training Policy* • Raytown Quality Schools, Security Awareness Program, Annual Security Training • Dysart Unified School District's student privacy training module is required as part of annual training. An internally developed system is connected to the courses in the LMS to track completion.
Security		
Foundational Information		
Require an internal and third party inventory of systems that collect and store student data	Checklist or related forms used in recording the inventory	CoSN Cybersecurity Resources • An Excel worksheet that can be used to inventory common system categories is available for downloaded from CoSN here. • CoSN Cybersecurity Self-Assessment • CoSN Cybersecurity Planning Rubric • CoSN Cybersecurity Planning Template
Account Management & Access		
Accounts and Passwords	Procedure and accompanying forms for provisioning, auditing accounts and revoking access	Account Request Procedure, Form • Baltimore County Public Schools *Guidance* • Note the special requirements for passwords when using student ID as an electronic identifier/username
Account access for non-employee workers • Interns/Student Teachers • Volunteers and Contractors	Account Request Procedure and accompanying form for provisioning access, auditing and deprovisioning access.	School Volunteers and FERPA (PTAC)
Systems Management		
Audits	Procedure for conducting security audits, across systems, including schedules and risk-management frameworks to be used when addressing audit findings.	*Resources* • Responding to IT Security Audits (PTAC) *Guidance* • HIPAA (Bozeman) • PCI (Fairfax) • Email (Baltimore County Public Schools (MD) policy, process
Data Governance		
Common components of a data governance policy include: • Policy and Procedure Oversight Responsibility • Data Stewards/Owners • Data Classification • Data Inventory • Data Storage		*Notes:* When developing your data governance policy, also consider specifying any unique requirements for both district and personal cloud computer storage, mobile device management and removable media that may be used in the school system, as well as implications of tools such as OneDrive, Google Backup and Sync, DropBox and related tools that sync local files to a cloud service.

Keep privacy top of mind.

Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies

Privacy Refresh

- Whether or not students create an account on the platform, remember that classroom activity is part of the education record, subject to legal protections.
- Audio containing an individual's voice is personal information, as is video containing an individual's likeness. All must be protected in accordance with federal and state law and your school system policies.
- If you permit chat functionality to be used, get clarity on how those will be transcribed and protect them accordingly. Note that "private chats" between a teacher and student are often captured as part of the full transcript and should also be protected as part of the education record.

CoSN Checklist

Assess the Privacy:

- Is use of the product in the classroom permissible under the operator's existing terms of service and privacy policy?
- What data will be shared with the technology provider? Have you verified that student personal information collected will only be used to support your educational purposes? When will it be deleted?
- If student data – including student images and voices – will be captured, have you identified all of the applicable student data privacy laws to consider?
- How will you use the product in compliance with your FERPA, CIPA and state student data privacy law obligations?
- Are you able to configure the product in a way that does not require students to create accounts?
- If the product will be used in classrooms where children are under the age of 13, how will the operator manage its COPPA obligations?
- Is the benefit to students outweighed by any questions about data protection?

Be transparent.

Build a Trusted Learning Environment with Parents

CoSN's Trusted Learning Environment Seal program (TLE) is designed to help school systems build, improve, and measure the maturity of their student data privacy practices against a framework designed specifically by and for school systems. The TLE program facilitates **clear, transparent communications** between school technology leaders, parents and other key community stakeholders about your commitment to protect student data.

Ensure that your school system is building trust with parents with these tips:

- Clearly communicate how your school system collects, manages, stores, and uses student data, authored by your superintendent or other administration leadership. Be sure the information is easy to find and easy to understand.
- Offer student data privacy and security training and related resources to parents at different points throughout the year. Educating stakeholders will help you have constructive conversations about education technology and how you protect student data privacy.
- Equip teachers with talking points that explain why student data is collected, how the use of technology benefits their child in the classroom, and how student data is used and protected.

> *"Educators will only gain the trust of parents and families if student information is used responsibly, ethically, and only when necessary to benefit students."*
> - Keith Krueger, CEO, CoSN

COSN
LEADING EDUCATION INNOVATION

Get Support Navigating the New Normal

COSN
LEADING EDUCATION INNOVATION

EdTech Guidance
In the age of COVID-19

Resources ▾ Solutions Directory ▾ Supporters About CoSN CoSN Home

EdTech Tools to Help You Navigate Uncharted Territory.

COSN
LEADING EDUCATION INNOVATION

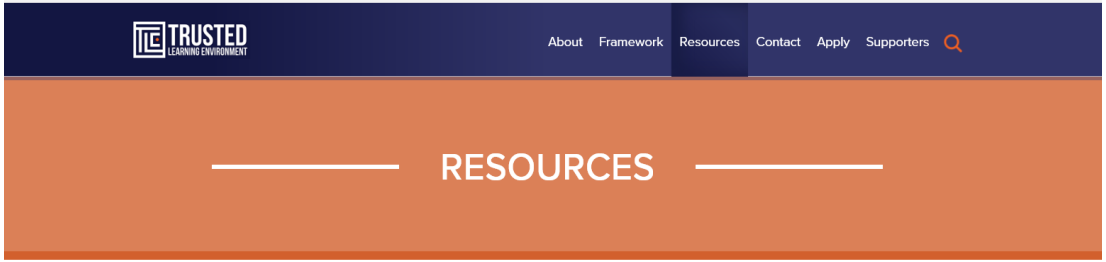
Start Today

Trusted Learning Environment Self-Assessment

Building Trust

- Take responsibility for bringing appropriate tech into your school system
- Provide proper education and training to employees, student and parents
- Demonstrate your competency
- Be transparent
- Continuously examine and improve your governance program

Privacy is never done. It's a discipline of ongoing improvement.



TLE Seal Program Handbook

The TLE Handbook explains how and why the TLE Seal Program was developed, and the benefits of participating. It also includes a...

DOWNLOAD

Before You Apply for the TLE Seal

Ready to apply, but not sure where to start? Download this Word Doc to find out more about what will be asked on the application.

DOWNLOAD

TLE Practices and Examples of Evidence

Need help in applying for the TLE? Download this resource for a list of examples that could be used as evidence for each of the TLE...

DOWNLOAD

Trusted Learning Environment Self-Assessment

Are you ready to apply for the TLE Seal? Take this self-assessment.

DOWNLOAD

Building a TLE Cohort in Your State

Working through the TLE Program can be complex, but you don't have to go it alone.

DOWNLOAD

TLE Seal Frequently Asked Questions

Here are the answers to some of the most commonly asked questions about the TLE Seal Program.

DOWNLOAD

TLE Seal Fact Sheet

Parents and other members of school communities are growing increasingly concerned about the protection...

TLE Webinar 2017

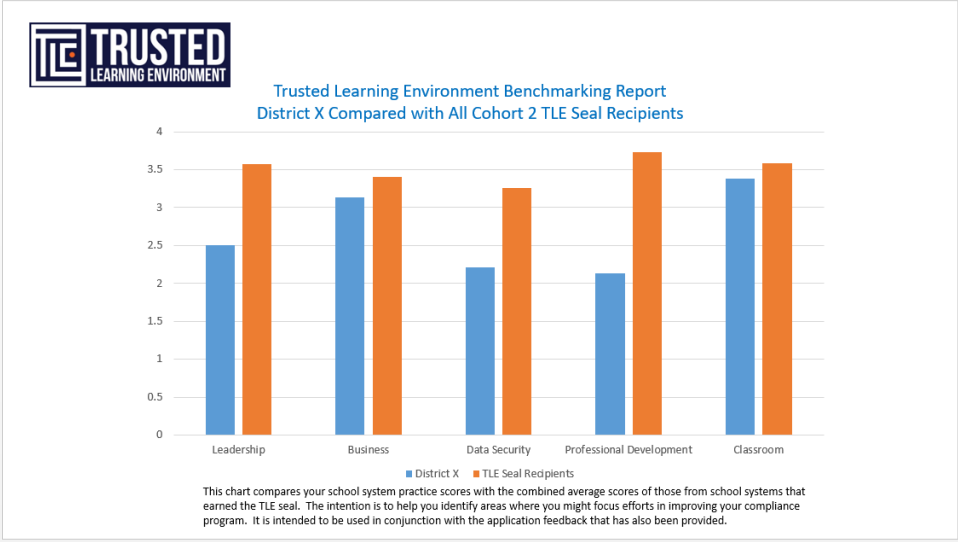
Follow Bob Moore, CIO Dallas ISD, and former TLE Project Lead, as he presents the Trusted Learning Environment to...

The Role of Leadership: Superintendents and Data Privacy

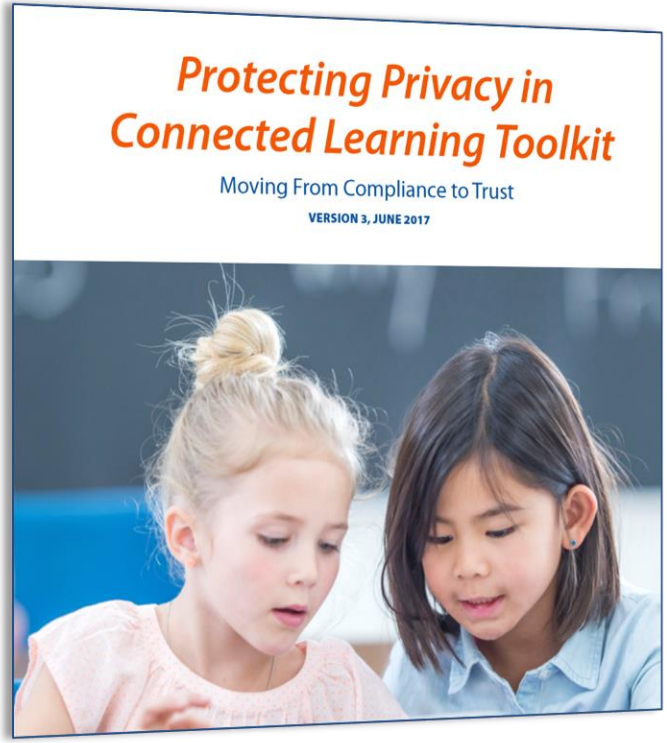
Developing a data privacy governance program is not the job of one person or one team. It is a multi-stakeholder...

Supporting Your Growth

- Customized feedback and recommendations
- Benchmarking
- Online privacy peer community
- Build trust in your community

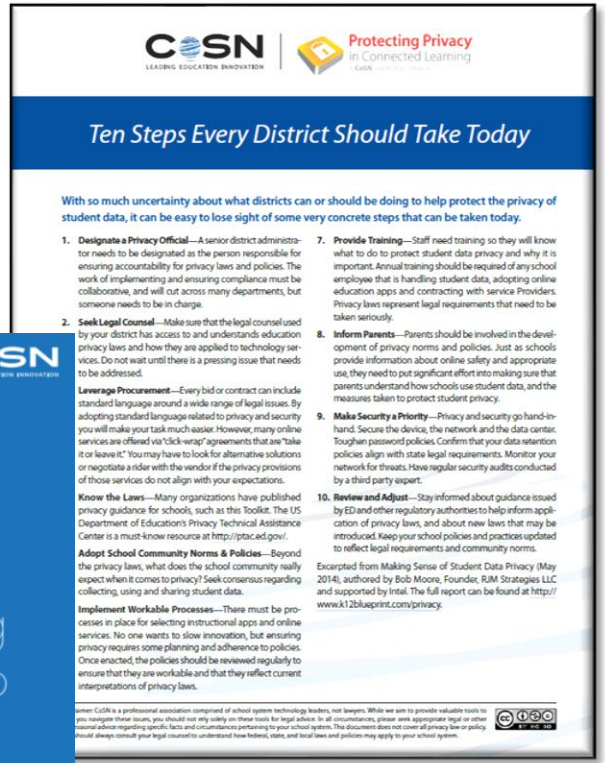


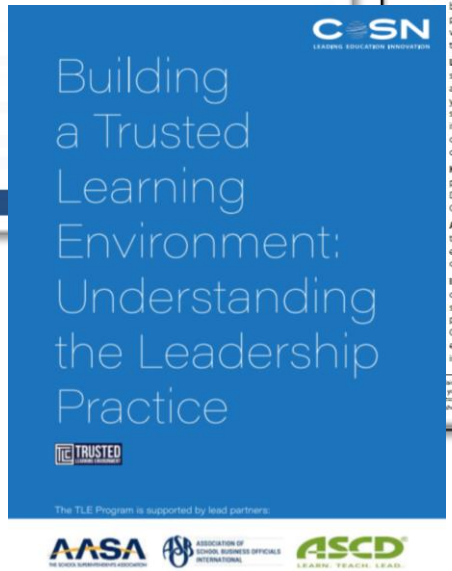
CoSN Resources



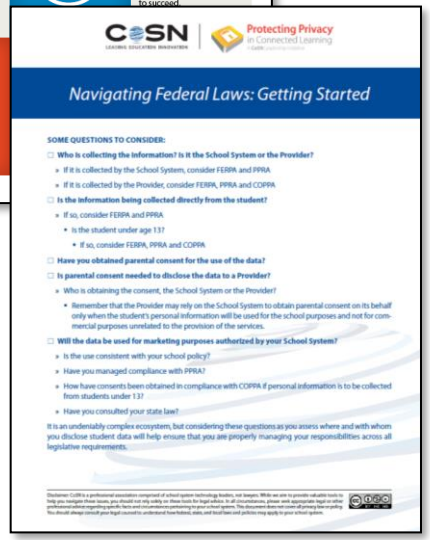
- FERPA & COPPA Decision Guide
- PPRA & HIPAA At-a-Glance
- Security Questions to Ask an Online Service Provider
- Suggested Terms for Contracts
- 10 Privacy Steps Every School District Should Take
- Communicating Privacy Practices Infographic (Developed with the National School Public Relations Association)
- Much more…


CoSN
LEADING EDUCATION INNOVATION
TRUSTED
LEARNING ENVIRONMENT
Student Data Privacy Roadmap:
Your Guide to Earning the TLE Seal


CoSN
LEADING EDUCATION INNOVATION
Protecting Privacy in Connected Learning
Ten Steps Every District Should Take Today
With so much uncertainty about what districts can or should be doing to help protect the privacy of student data, it can be easy to lose sight of some very concrete steps that can be taken today.
1. Designate a Privacy Official—A senior district administrator needs to be designated as the person responsible for ensuring accountability for privacy laws and policies. The work of implementing and ensuring compliance must be collaborative, and will cut across many departments, but someone needs to be in charge.
2. Seek Legal Counsel—Make sure that the legal counsel used by your district has access to and understands education privacy laws and how they are applied to technology services. Do not wait until there is a pressing issue that needs to be addressed.
Leverage Procurement—Every bid or contract can include standard language around a wide range of legal issues. By adopting standard language related to privacy and security you will make your task much easier. However, many online services are offered via "click-wrap" agreements that are "take it or leave it." You may have to look for alternative solutions or negotiate a rider with the vendor if the privacy provisions of those services do not align with your expectations.
Know the Laws—Many organizations have published privacy guidance for schools, such as this Toolkit. The US Department of Education's Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.
Adopt School Community Norms & Policies—Beyond the privacy laws, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing student data.
Implement Workable Processes—There must be processes in place for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to policies. Once enacted, the policies should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws.
7. Provide Training—Staff need training so they will know what to do to protect student data privacy and why it is important. Annual training should be required of any school employee that is handling student data, adopting online education apps and contracting with service Providers. Privacy laws represent legal requirements that need to be taken seriously.
8. Inform Parents—Parents should be involved in the development of privacy norms and policies. Just as schools provide information about online safety and appropriate use, they need to put significant effort into making sure that parents understand how schools use student data, and the measures taken to protect student privacy.
9. Make Security a Priority—Privacy and security go hand-in-hand. Secure the device, the network and the data center. Toughen password policies. Confirm that your data retention policies align with state legal requirements. Monitor your network for threats. Have regular security audits conducted by a third party expert.
10. Review and Adjust—Stay informed about guidance issued by ED and other regulatory authorities to help inform application of privacy laws, and about new laws that may be introduced. Keep your school policies and practices updated to reflect legal requirements and community norms.
Excerpted from Making Sense of Student Data Privacy (May 2014), authored by Bob Moore, Founder, RJM Strategies LLC and supported by Intel. The full report can be found at http://www.k12blueprint.com/privacy.


CoSN
LEADING EDUCATION INNOVATION
Building a Trusted Learning Environment: Understanding the Leadership Practice
TRUSTED
The TLE Program is supported by lead partners:
AASA
THE SCHOOL SUPERINTENDENTS ASSOCIATION
ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL
ASCD
LEARN. TEACH. LEAD.


Our Commitment to You:
CLEAR PRIVACY PRACTICES
Parents and guardians want assurances that personal information and data about their children are secure and protected by our school system. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning and new technologies to deliver exciting new education services.
At our school, we strive to be clear about what data we collect, how data support your child's education and the safeguards in place to protect that data.
What Data do We Collect and Why?
Address
School Operations
We collect data such as addresses and phone numbers, gender and age, as well as information to ensure student safety and accurate reporting to help run our school operations efficiently.
Measuring Progress and Participation of our Students
We collect data such as attendance, grades and participation in school-sponsored extra-curricular activities to enable students to succeed.
Improving the Education Program
We collect results from local, state and national assessments to provide teachers, administrators and parents important information about student, program and school performance and improve the education programs we offer.


CoSN
LEADING EDUCATION INNOVATION
Protecting Privacy in Connected Learning
Navigating Federal Laws: Getting Started
SOME QUESTIONS TO CONSIDER:
Who is collecting the information? Is it the School System or the Provider?
If it is collected by the School System, consider FERPA and PPRA
If it is collected by the Provider, consider FERPA, PPRA and COPPA
Is the information being collected directly from the student?
If so, consider FERPA and PPRA
Is the student under age 13?
If so, consider FERPA, PPRA and COPPA
Have you obtained parental consent for the use of the data?
Is parental consent needed to disclose the data to a Provider?
Who is obtaining the consent, the School System or the Provider?
Remember that the Provider may rely on the School System to obtain parental consent on its behalf only when the student's personal information will be used for the school purposes and not for commercial purposes unrelated to the provision of the services.
Will the data be used for marketing purposes authorized by your School System?
Is the use consistent with your school policy?
Have you managed compliance with PPRA?
How have consents been obtained in compliance with COPPA if personal information is to be collected from students under 13?
Have you consulted your state law?
It is an undeniably complex ecosystem, but considering these questions as you assess where and with whom you disclose student data will help ensure that you are properly managing your responsibilities across all legislative requirements.

Partners

Lead Partners

AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

ASBO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

ASCD LEARN. TEACH. LEAD.

Additional Partners

CCSSO Council of Chief State School Officers

DQC DATA QUALITY CAMPAIGN

FUTURE READY SCHOOLS

FUTURE OF PRIVACY FORUM

iKeepSafe

naesp

NASSP National Association of Secondary School Principals

NASBE National Association of State Boards of Education

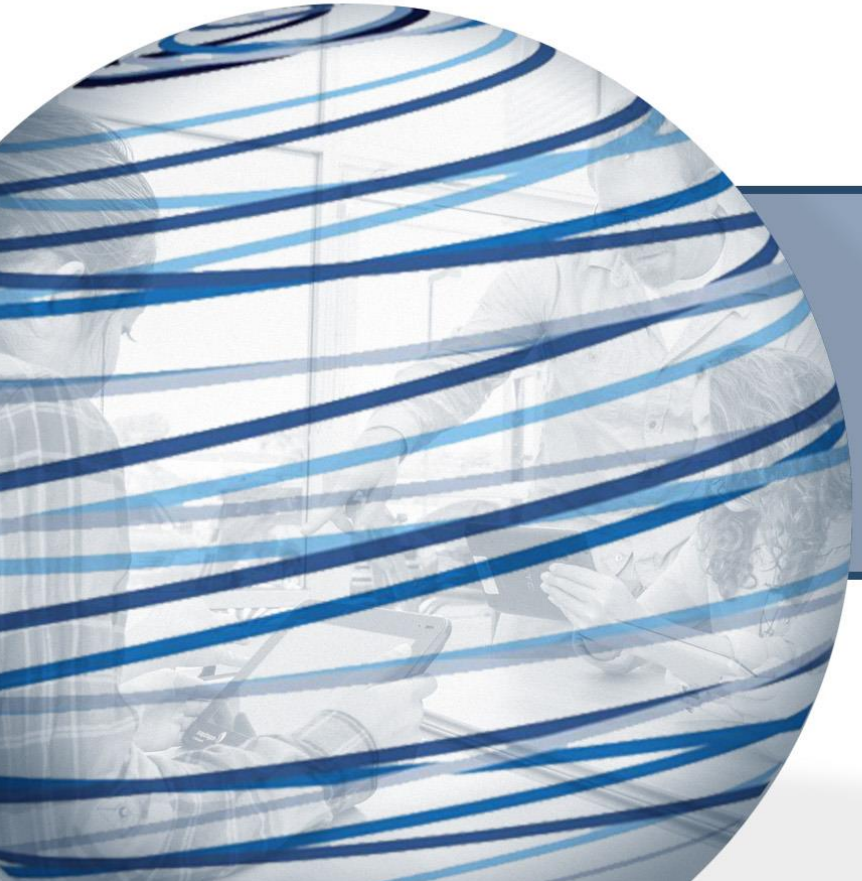
PDK

StriveTogether Every child. Cradle to career.

Thank You | Corporate Partners

Amazon Web Services
CDW.G
Cisco
ClassLink
Clever
ContentKeeper Technologies
Dell Technologies
Diamond Assets
Ed-Fi Alliance
ENA/CatchOn
FileWave
Fortinet
Google for Education
HP
iboss
Identity Automation
Juniper Networks
Kajeet
Lenovo
Lightspeed Systems
ManagedMethods
Pearson
SAFARI Montage
SHI International
Verizon

Questions?



LEADING EDUCATION INNOVATION

Thank You

Linnette Attai
Project Director, CoSN Protecting Privacy Initiative and Trusted Learning Environment Program
LAttai@cosn.org