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

Introductions

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 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 7277083

Is your district currently...

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>In person learning only</td>
<td>Remote learning only</td>
<td>Hybrid</td>
<td>Hybrid and parents can change their choice throughout the year.</td>
</tr>
</tbody>
</table>
What are your most pressing privacy concerns in remote or hybrid learning environments?
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
# Build Your Foundation

**Behavior, guided by policy, backed by procedure.**

## Training

<table>
<thead>
<tr>
<th><strong>Policy requiring periodic privacy and security training for staff with access to education records</strong></th>
<th><strong>Process for maintaining record of training</strong></th>
<th><strong>Example Training Policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Raytheon Quality Schools, Security Awareness Program, <a href="#">Annual Security Training</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Project: Unified School District's student privacy training module</a> is required as part of annual training. An internally developed system is connected to the courses in the LMS to track completion.</td>
</tr>
</tbody>
</table>

## Security

### Foundational Information

<table>
<thead>
<tr>
<th><strong>Require an internal and third party inventory of systems that collect and store student data</strong></th>
<th><strong>Checklist or related forms used in recording the inventory</strong></th>
<th><strong>CoSN Cybersecurity Resources</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- An Excel worksheet that can be used to inventory common system categories is available for downloaded from <a href="#">CoSN here</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">CoSN Cybersecurity Self-Assessment</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">CoSN Cybersecurity Planning Public</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">CoSN Cybersecurity Planning Template</a></td>
</tr>
</tbody>
</table>

### Account Management & Access

<table>
<thead>
<tr>
<th><strong>Accounts and Passwords</strong></th>
<th><strong>Procedure and accompanying forms for provisioning, auditing accounts and revoking access</strong></th>
<th><strong>Account Request Procedure, Form</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Baltimore County Public Schools</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Note the special requirements for passwords when using student ID as an electronic identifier/username.</td>
</tr>
</tbody>
</table>

### Account access for non-employee workers

- Teachers/Student Teachers
- Volunteers and Contractors

<table>
<thead>
<tr>
<th><strong>Account Request Procedure and accompanying forms for provisioning access, auditing and deprovisioning access.</strong></th>
<th><strong>School Volunteers and FERPA (PTAC)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Systems Management

### Audits

<table>
<thead>
<tr>
<th><strong>Procedure for conducting security audits, across systems, including schedules and risk management frameworks to be used when addressing audit findings.</strong></th>
<th><strong>Responding to IT Security Audits (PTAC)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Governance

<table>
<thead>
<tr>
<th><strong>Common components of a data governance policy include:</strong></th>
<th><strong>Notice</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Policy and Procedure Oversight Responsibility</td>
<td></td>
</tr>
<tr>
<td>- Data Stewards/Owners</td>
<td></td>
</tr>
<tr>
<td>- Data Classification</td>
<td></td>
</tr>
<tr>
<td>- Data Inventory</td>
<td></td>
</tr>
<tr>
<td>- Data Storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>
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
Get Support Navigating the New Normal

EdTech Tools to Help You Navigate Uncharted Territory.
Start Today

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.
Supporting Your Growth

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

This chart compares your school system practice scores with the combined average scores of those from school systems that earned the TLE seal. The intention is to help you identify areas where you might focus efforts in improving your compliance program. It is intended to be used in conjunction with the application feedback that has also been provided.
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…
Ten Steps Every District Should Take Today

With so much uncertainty about where 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 Officer—A barrier to detection is training 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 the person designated must have the guidance and management skills required.

2. Seek Legal Counsel—Make sure that the legal counsel used by your district has access to and understands education privacy law and how they apply to educational technology services. Do not wait until there is a pressing issue that needs to be addressed.

3. Leverage Procurement—Every bid for contract includes standard language around needs ranges of legal issues. By adopting standard language related to privacy and security you will reduce your legal risk easier. However, many vendors list services on their site that are "How to Use It". You may have to look at different solutions or negotiate a contract with the vendor if the privacy provisions of these services do not align with your expectations.

4. Know the Law—Many organizations have published privacy guides for schools, such as this toolkit. The US Department of Education’s Privacy Technical Assistance Center is a must-know resource at https://ope.ed.gov.

5. Adjust School Community Norms & Policies—Beyond the privacy law, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing data.

6. Implement School Policies—There must be policies in place for selecting instructional apps and online services. For new ones we are slow to react, 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 circumstances of privacy law.

What data do we collect and why?

- Building a Trusted Learning Environment: Understanding the Leadership Practice
- Navigating Federal Laws: Getting Started
- Protecting Privacy in Connected Learning

Parents and guardians want assurance 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.
Partners

Lead Partners

Additional Partners
<table>
<thead>
<tr>
<th>Amazon Web Services</th>
<th>Ed-Fi Alliance</th>
<th>Juniper Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDW.G</td>
<td>ENA/CatchOn</td>
<td>Kajeet</td>
</tr>
<tr>
<td>Cisco</td>
<td>FileWave</td>
<td>Lenovo</td>
</tr>
<tr>
<td>ClassLink</td>
<td>Fortinet</td>
<td>Lightspeed Systems</td>
</tr>
<tr>
<td>Clever</td>
<td>Google for Education</td>
<td>ManagedMethods</td>
</tr>
<tr>
<td>ContentKeeper Technologies</td>
<td>HP</td>
<td>Pearson</td>
</tr>
<tr>
<td>Dell Technologies</td>
<td>iboss</td>
<td>SAFARI Montage</td>
</tr>
<tr>
<td>Diamond Assets</td>
<td>Identity Automation</td>
<td>SHI International</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verizon</td>
</tr>
</tbody>
</table>
Questions?
Thank You

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