



# Protecting Student Data Can Be A Perilous Journey



# Presenters



**Connie Coy**

MOREnet



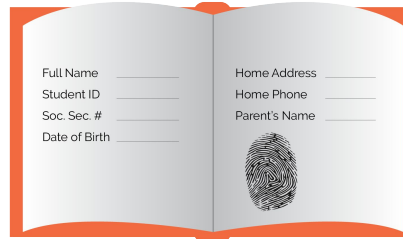
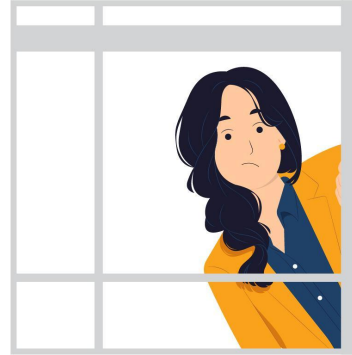
**Ramah Hawley**

The Education  
Cooperative (TEC)

# Integrating Privacy into Cybersecurity

# SDP and Cybersecurity

Hand in Hand



# Incorporating SDP

MOREnet Web Pages

Blog

Cybersecurity Trainings Onsite

MOREnet Conferences/ Technical Summit

Cybersecurity Assessments Onsite

Incident Response Plan Tabletop Onsite

Webinars – Ask the Expert

Data Minimization – The Most Secure Data is the Data You Don't Have



Directory Information Exception – What Districts Need to Know



# Incorporating SDP

## Privacy Best Practices



When developing a data privacy program, there are a variety of steps that will make setting this up run smoothly. Determining why your organization needs a program, what should be included in a program and how to go about creating one should all be considered.

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a one-stop resource to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at <http://studentprivacy.ed.gov>.

Their [Checklist for Developing School District Privacy Programs](#) can be utilized as you are just getting started. It gives a good overview of how to work through the process of setting up a program.

The [Data Governance Checklist](#) can assist your organization with establishing and maintaining a successful data governance program to help ensure the individual privacy and confidentiality of records.

Use the steps below to implement your privacy program!

- ✦ Step One: Policies for Users of Student Data Checklist
- ✦ Step Two: Data Minimization
- ✦ Step Three: Inventory Worksheet
- ✦ Step Four: Data Classification Guide
- ✦ Step Five: Mapping Data Flows Checklist
- ✦ Step Six: Data Destruction Document

## Student Privacy



Student data privacy diligence is a continual concern for all educators. To assist our members with this critical effort, MOREnet has partnered with the Student Data Privacy Consortium (SDPC) to establish the Missouri Student Privacy Alliance (MOSPA). **This service is available to MOREnet K-12 Full and Basic Members and included in their service package at no additional fee.**

[Join MOSPA >>](#)

MOSPA, in conjunction with the SDPC, provides K-12 members tools and resources to ensure student data is protected in the districts. The goal is to provide common expectations between the district and vendor and streamline the agreement process.

In addition to MOSPA, members have the opportunity to take advantage of the managed services of The Education Cooperative (TEC). TEC Service provides many resources to help schools ensure student data privacy, helping to increase compliance and reduce member school's workload.

K-12 members have several avenues to ensure student data privacy:

### Option One: No standardized privacy agreement

Districts independently adopt a student data privacy agreement with each vendor that uses or collects personally identifiable information or obtain parental permission to use the application. This leads to time consuming and costly work without uniformity and order. See our [blog about the importance of data privacy](#).

### Option Two: Become a Missouri Student Privacy Alliance (MOSPA) member

A free service for MOREnet members that allows access to the Student Data Privacy Consortium (SDPC) tools and resources. This includes a searchable database of national and state agreements and training. MOSPA members will have access to the MO National Data Privacy Agreement to provide uniformity in agreements with vendors throughout the state. MOREnet will provide training and support for using the platform. [Learn more and become a member.](#)

### MOSPA & The Education Cooperative (TEC)

After joining MOSPA, a member may elect to take advantage of the managed services of TEC for a reasonable annual fee. In addition to option two, this fee-based selection takes the negotiation process out of your hands. MOSPA/TEC provides MO NDPA agreement processing, vendor negotiation, and inherent legal services. This process greatly reduces the district's time in processing and negotiating and opens the door to hundreds more agreements. TEC currently has 1800+ agreements and is continually adding agreements. [Learn more about the MOSPA/TEC partnership.](#)

# Cybersecurity Assessment

ASSESSMENT SUMMARY:	
Area	Score %
Physical Security	83
Network Infrastructure	79
Secure Configurations	72
Access Control	83
Monitoring	75
Enterprise Asset Inventory	75
Data Lifecycle Handling	35
Network & Endpoint Protections	83
Data Protection and Recovery	80
Policies	27
Training	67
Passwords	42
<b>TOTAL</b>	<b>67</b>

## Your Cybersecurity Posture is: Very Good

Our assessment is based on Security Best Practices, CIS Critical Controls and NIST Cybersecurity Framework. You will need to evaluate your individual level of risks associated with vulnerabilities and deficits sited in this report. This report should serve as a baseline for areas of strength and concern to improve your overall security defenses.



Total Score | Excellent: 80-100% | Very Good: 60-79% | Good: 40-59% | Fair: 20-39% | Poor: Less than 20

Data Lifecycle Handling	Findings	Recommendations:
<p>CIS Control 3-Data Protection Establish and communicate policies and procedures for handling records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying data.</p>	<ol style="list-style-type: none"> <li>-Annual notice is sent to parents/patrons about their rights under the Family Educational Rights and Privacy Act (FERPA).</li> <li>-We have a vetting process and agreements with service providers addressing expectations of the handling and use of sensitive data.</li> <li><b>The organization does not maintain an inventory of sensitive information</b></li> <li>There is a documented process for vetting software and extensions in relation to the release and responsibility to PII</li> <li>There is no written policy on data retention. (CIS 3.4)</li> <li>Do not have a documented process for the removal of sensitive information.</li> </ol>	<ol style="list-style-type: none"> <li>Meets Standard(s)</li> <li>Meets Standard(s)</li> <li><b>To create a data inventory and catalog, start by identifying all data sources within your organization, including databases, cloud storage, and external data sets. Document the type, location, format, and ownership of each data source.</b></li> <li>Meets Standard(s)</li> <li>Lacking specific guidance to dictate the length of retention of data from production systems, enterprise data can become cumbersome to manage, which may lead to accidental data loss or mismanagement. The state of Missouri has a</li> </ol>
<p><b>Score</b> <b>35%</b></p>		

# Incorporating SDP

Cybersecurity News Review – add any general SDP information and routinely advertise MOSPA Service.

Bi-monthly MOSPA Newsletter – specific to our MOSPA members include SDPC Webinars, Presentations

MOSPA Leadership Team Meetings – Monthly

MOSPA Member Meetings – 5-6 Annually

TEC Recently Renewed and Newly Signed DPAs sent Monthly

# MOSPA Newsletter



## MOSPA

Missouri Student Privacy Alliance

It's Data Privacy Week! A great time to revisit the resources and tools available to you through your membership in the MOREnet Consortium.



Mark Your Calendar!  
Helpful Webinars Scheduled

Training opportunities from the National Student Data Privacy Consortium (SDPC).

January 28, 2026, 1 p.m.

[Less Data Collected, Less Data Exposed](#)

January 30, 2026, 1 p.m.

[Ready to Answer: How the SDPC Helps Schools Respond to Privacy Challenges](#)



### Important SDPC Resource Registry Information

Please use the View **Expiring** Agreement option only. The View **Expired** Agreements will incorrectly allow you to request agreements that have Exhibit Es available and/or if you have an updated agreement in place.

## Resource Registry Instructions for Parental Consent

We love getting your questions and feedback! Recently, we were able to help with this request from a district "We have signed parental consent forms for HUDL use and access for players. I would like help with adding an agreement like other districts have in place."

Below are the instructions.

Company Name	Resource Name	Date Approved	Expires on	Agreements
Agile Sports Technologies, Inc.	<a href="#">HUDL</a>	2025-08-01	2028-07-31	Legal Drafted Guardian Release

# Rough Waters

- Student data privacy awareness in district
  - Goal is to protect student data
  - Build Community Trust/Due Diligence
  - Provides a nationally recognized student data privacy legal agreement (NDPA) utilizing the School Official Exception/based on FERPA
  - Teachers are Partners – Find an advocate
  - Administrative Buy-in

# Rough Waters

- Internal Vetting Process
- Directory Information Exception
- Extra-curricular activities applications
- Staffing time

## Developing an Internal Vetting Process

**Goal:** The district has a National Data Privacy Agreement (NDPA) for every resource that has access to student Personally Identifiable Information (PII).

**Assemble a software vetting team with these roles:**

- Privacy
- Budgetary
- Technical
- Curriculum

**Create an inventory of software applications**

**Prioritize resources to pursue NDPA**

- Sensitivity of data
- Scope of use
- Upcoming renewals
- New purchases (RFP-NDPA)
- Pilot programs

**Ask if use of the software application aligns with the district's educational goals and policies.**

## Student Data Privacy & FERPA What Coaches Need to Know

As a coach, you play a key role in protecting student privacy. Here's a guideline of what you can and can't share under FERPA and the standard privacy policies when using digital tools or posting team content.

**You Can Share the Following Information:** Unless the family doesn't allow it:

- These can be considered **directory information**: check with your district policy:
  - Student names, age, and grade level
  - Participation in sports or activities
  - Team photos and videos
  - Height and weight for athletes
  - Performance data (e.g., stats, scores, game highlights)
  - Honors and awards received
  - Recorded sound or images, as long as it's not harmful or invasive

**Important:** There can NOT be shared publicly (e.g., Hall, team social media accounts) if the family has opted out of directory information sharing.

**You May NOT Share the Following Without Parental Consent:**

- Any **student information** (including directory info) for families who **opted out**
- Private** team notes, evaluations, or behavioral observations
- Health or injury information**
- Academic data** (grades, eligibility status)
- Anything that could be considered harmful or invasive

**Using Team Management Apps:**

Apps for team management may only be used by teams within these guidelines:

- Content must follow FERPA guidelines
- Parent permission forms must be signed
- Public team pages should be managed carefully
- Non-directory information not shared (like notes, academic info)
- Private team access unless cleared by admin

Any app or software that contains player information must be approved by an administrator. Check with your athletic director and technology services team to determine who that is of your school who protects student records.

**Know Who Opted Out:**

Families who OPT OUT do not want their child's data shared. **Before posting names, stories, photos, or video highlights on websites, apps, or social media:**

- Check with your admin for a list.

**Before sharing or importing student information with third party vendors:**

- Confirm a student data privacy agreement has been signed, or follow the process to obtain parent permission.

Work with administrative or SIS staff who can assist with checking family preferences.

**Think of It This Way:**

Media inclusion is like a student saying "Start just my picture on the wall."

**Vendor data sharing is like giving that picture to a company who can make copies, analyze it, or even share it with partners—unless it has been locked down with them.**

## What Coaches Need to Know About Student Data Privacy



# Developing a Crew

## SDPC

University of MO Legal Counsel

## District Security/Technical Contacts

- Curriculum Instructors
- Purchasing Dept

MOSPA Leadership Team

## TEC

DESE – MSIP6

K-12 Insurance Provider(s)

School Board Association

Superintendent Conferences

Student Athletic Activities Association

MO SOS Records Retention

University of MO Data Governance

MOREnet Staff/Staff Meetings

A4L Quarterly – **MOREnet Admin**

MOSPA/TEC School Districts

# Gaining a Foot Hold

Determining areas - Statewide map

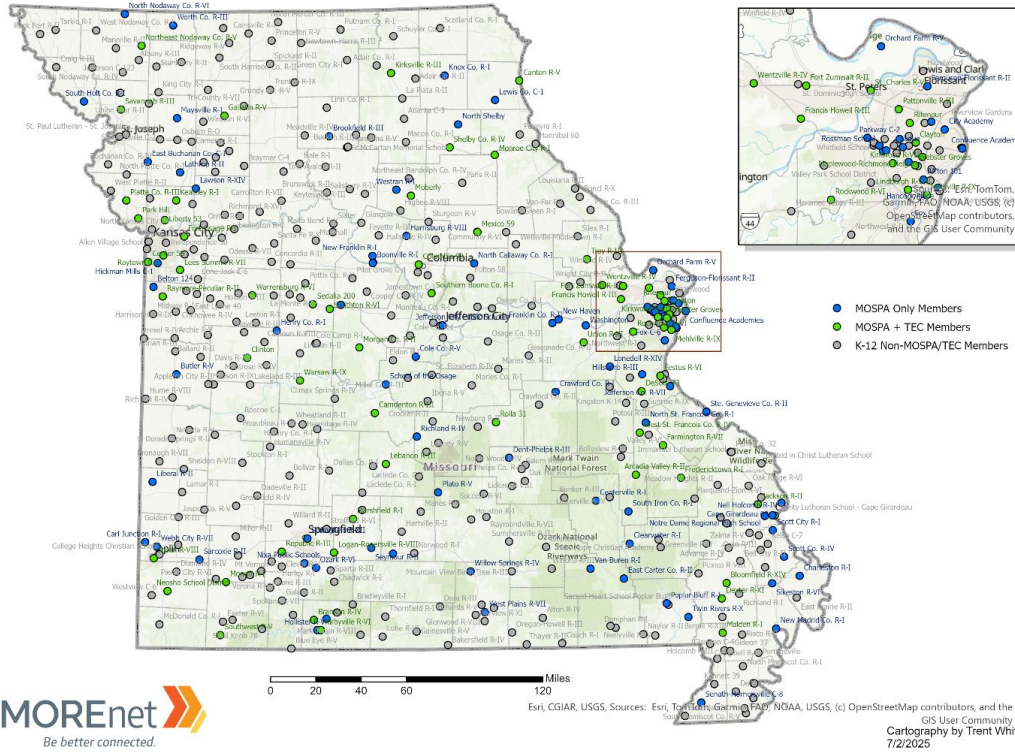
SDP Regional Discussions

The “Domino” District

MOREnet Member Services Representative



### MOSPAs Members



# SDP Regional – Two Hours

- 15 Minute SDPC Overview
- 30-45 Min MOSPA Districts sharing their journey
- 30 Min TEC Presentation
- Roundtable/Answer Questions

# Successes

## TEC

Success Ready Students – Marzano Dashboard Vendor

Lightspeed – promotes SDPC/MOSPA at districts

## MOREnet

Vendors at MOREnet Conferences – thank the vendors that have signed the NDPA.

Districts that have persuaded vendors to sign

# Challenges

Organizations that purchase software for districts and are unwilling to sign the NDPA.

Getting the right people from the organizations together to discuss when there are multiple Purchasing layers

Continue to have the conversations and Never Give Up!

# Tough Questions

A third-party attorney doesn't believe the Exhibit E subscription process is legal. How do I respond?

I use a third-party tool to initially vet resources and sometimes there are indicators of concern, but I see there is a signed data privacy agreement. How do these two things correlate?

How do I process an agreement when the product is purchased by a State-wide entity? Who signs the NDPA as the vendor?

The legal name of the district is different than the "common State name".

# MOREnet SDP Resources

[Privacy Best Practices](#)

[Student Privacy](#)

[Data Minimization – The Most Secure Data is the Data You Don't Have](#)

[Directory Information Exception – What Districts Need to Know](#)

[What Coaches Need to Know About Student Data Privacy](#)

[Guide for Developing an Internal Vetting Process](#)

# Student Data Privacy Resource

[A District Guide to Data Minimization in the Age of AI](#)

[How to Quickly Spot Red Flags in Privacy Policies](#)

[The Policymaker's Guide to Student Data Privacy](#)

[Agent FERPA – Security Training for Teachers](#)



# Questions?

**Thank you for attending!!**