Trusted Learning Environment (TLE) in PHSD 23

December 18, 2025

TLE: "Don't Go Chasing Waterfalls"

CERTIFICATE of ACHIEVEMENT

THIS ACKNOWLEDGES THAT

Prospect Heights School District 23

HAS SUCCESSFULLY EARNED THE

Trusted Learning Environment Mini-Seal in Leadership

AS PART OF THEIR STRONG COMMITMENT TO PROTECTING STUDENT DATA PRIVACY

Keith Krueger
CEO, Consortium for School Networking

In the past, the District has had separate, formal Technology Plans to track goals around curriculum and instruction, safety, and replacement cycles and budgeting. Technology is so ubiquitous in every department now that we plan for and track technology needs through integration into each department. For example, Curriculum and Instruction considers artificial intelligence (A.I.) use in curricular tools, and the District budget considers iPads and laptops as necessary devices.

One way we do see our work is through the Trusted Learning Environment (TLE) Seals

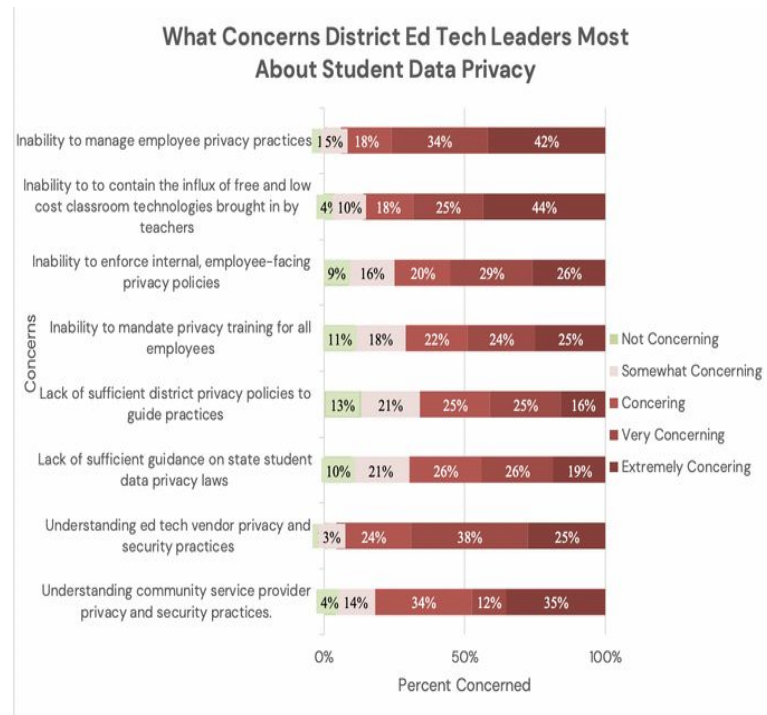## About the CoSN Trusted Learning Environment Seal Program

The CoSN Trusted Learning Environment (TLE) Seal program is the nation's only data privacy framework for school systems, focused on building a culture of trust and transparency. The TLE Seal was developed by CoSN in collaboration with a diverse group of 28 school system leaders nationwide and with support from AASA, The School Superintendents Association, the Association of School Business Officials International (ASBO) and ASCD. School systems that meet the program requirements will earn the TLE Seal, signifying their commitment to student data privacy to their community. TLE Seal recipients also commit to continuous examination and demonstrable future advancement of their privacy practices. CoSN.org/Trusted

#PROUD2BD23 SCHOOL PRIDE

What Does TLE Mean for Us?

Long-standing best practices about student data privacy and safety; the COVID-era proliferation of programs; equity concerns around digital skills and support at home; and questions about the different types of screen time for children have led to this moment to curate safe learning experiences for students!

What Concerns District Ed Tech Leaders Most About Student Data Privacy
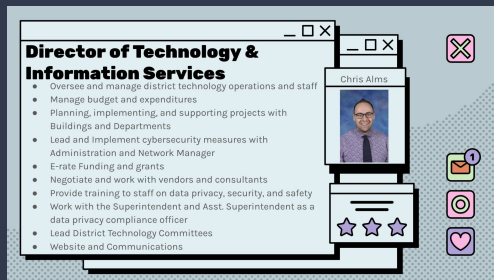
Additions to Core Curricula

Our curriculum committees and instructional coaches have put in a lot of time to offer myriad resources to maximize our core curricula. With that, we know there are new programs that can support engagement and assessment needs. If you are requesting a new program to be used to support student learning, you will follow the steps in the Procedure for Requesting a Digital Resource

For a user-friendly walk through, see this presentation, Requesting an App/Program

Privacy and Safety Requirements

Program Approval

Any program we use that collects student personally identifiable information (PII) must be approved!

Any program we use to enhance learning and the learning environment for students must be safe, support Board-approved curricula, and be sustainable from a cost perspective.

Link to our formal procedure, HERE

Link to the presentation for how to request, HERE

CIPA- Children's Internet Protection Act - must monitor online activities of minors, educate minors regarding appropriate online behavior, and establish a safety policy; also filters/blocks Internet access to inappropriate sites and images.

FERPA- Family Educational Rights and Privacy Act – protects the privacy of student education records. Provides parents right to inspect file and make corrections.

COPPA- The Children's Online Privacy and Protection Act - deals with how websites, apps, and other online operators collect data and personal information about kids under the age of 13.

SOPPA- Student Online Personal Protection Act - protects student data collection by educational technology companies and confirming data is used for educational purposes only.

D23 App/Program Approval Meeting							
Date							
App/Program Name							
Approval Team Member Attendance (Check above Name)		☐	☐	☐	☐	☐	☐
All programs must support Board-approved curricula, be safe, and follow necessary data-privacy requirements.							
Approval Team Members (Each team member provides feedback here)		Data Privacy Officer	Assistant Superintendent of C & I	Technology Integration Specialist (TIS)	Principal:	Instructional Coach:	Tech Connect 1:
Purpose/Integrity of Core Curriculum							
Purpose of the App							
What Need Does This Meet?							
How Does This Support the Core Curriculum?							
In What Grades and Subjects Would This Be Used?							
Are There Further Needs for Sped/ML Students?							
Privacy/Safety							
What Is the Education Framework Privacy Score?							
Why Did the App/Program Earn That Score?							
What Student Information Is Collected by the Vendor?							
What Is the Minimal Amount of Information from Students Needed for Them to Use This App/Program?							
Is There Already an Originating SOPPA Agreement?							
If "Yes," Is There Any Language in Exhibit H That Contradicts Our Safety Needs?							
If "No," What Does the Vendor Say When Contacted?							
Is This Program Available on the Clever DashBoard?							
Cost							
What Is the Cost Structure? (If this is a free app/program, write that here and skip the rest of this section.)							
Are There Programs That Could Be Reduced in Need Due to What This Program/App Does?							
Are There Known Discounts for Contracts?							
Final Status							
Approved							
Considered, with Questions							
Denied							

TLE: Leadership

District and building leaders understand data privacy and security, actively support a system of processes, and communicate transparently about these processes, policies, and procedures.

Our A.I. guidelines, spurred by State Senate Bill 1920, exist under this leadership domain.

SPRING BREAK iPAD TURN IN

UPDATE YOUR IPAD AND BE READY TO TURN IT IN BEFORE SPRING BREAK!

Director of Technology & Information Services
- Oversee and manage district technology operations and staff
- Manage budget and expenditures
- Planning, implementing, and supporting projects with Buildings and Departments
- Lead and Implement cybersecurity measures with Administration and Network Manager
- E-rate Funding and grants
- Negotiate and work with vendors and consultants
- Provide training to staff on data privacy, security, and safety
- Work with the Superintendent and Asst. Superintendent as a data privacy compliance officer
- Lead District Technology Committees
- Website and Communications

Chris Alms

#PROUD2BD23 SCHOOL PRIDE

Technology Department

Student Online Data Privacy

Student Online Personal Protection Act (SOPPA)

District 23 takes the privacy and online safety of our students very seriously. We have always taken steps to guard closely the student data collected within our networks or by the online resources we use in our schools. Effective July 1, 2021, all school districts will be required by the Student Online Personal Protection Act (SOPPA) to provide additional guarantees that student data is protected when collected by educational technology companies and that the data is used for beneficial purposes only. The goal of SOPPA aligns with the goal of D23: increase transparency, protect student data, and protect students.

Annual Notice to Parents about Educational Technology Vendors Under Student Online Personal Protection Act

D23's Approved Online Resources

The list includes the online services or applications that the District uses, the contracts signed by the District, and any data collected by those tools or by the District. The District regularly updates and verifies applications and tools. Teachers and staff can review the District process for requesting a program HERE. Teachers and staff can fill out this form to request the District to verify if an application or tool is SOPPA compliant.

Privacy and Safety Requirements

Program Approval

Any program we use that collects student personally identifiable information (PII) **must be approved!**

Any program we use to enhance learning and the learning environment for students must be safe, support Board-approved curricula, and be sustainable from a cost perspective.

Link to our formal procedure, HERE

Link to the presentation for how to request, HERE

CIPA- **Children's Internet Protection Act** - must monitor online activities of minors, educate minors regarding appropriate online behavior, and establish a safety policy; also filters/blocks Internet access to inappropriate sites and images.

FERPA- **Family Educational Rights and Privacy Act** - protects the privacy of student education records. Provides parents right to inspect file and make corrections.

COPPA- **The Children's Online Privacy and Protection Act** - deals with how websites, apps, and other online operators collect data and personal information about kids under the age of 13.

SOPPA- **Student Online Personal Protection Act** - protects student data collection by educational technology companies and confirming data is used for educational purposes only.

Using AI Responsibly in District 23 Schools

Our Guiding Principles

Purpose-Driven
We use AI to help all students achieve their educational goals.

Balanced Approach
We work to realize the benefits of AI while addressing risks like misinformation.

Upholding Integrity
Honesty, trust, and fairness are expectations for all students and staff.

Human-Centered Agency
People, not AI, are responsible and accountable for all final decisions.

AI in Practice: A Quick Guide

DO: Spark Student Creativity

Students can use AI to brainstorm, aid in writing, and create visual arts.

DO: Support Staff & Teachers

Staff can use AI to differentiate lessons, design assessments, and draft communications.

DON'T: Plagiarize or Cheat

DON'T: Plagiarize or Cheat. Submitting AI-generated work as original work is strictly prohibited.

DON'T: Compromise Privacy

confidential

DON'T: Compromise Privacy. Never enter confidential or personally identifiable information into AI tools.

DON'T: Bully or Harass

DON'T: Bully or Harass. Using AI to impersonate or intimidate others is strictly forbidden.

Of Note(book)
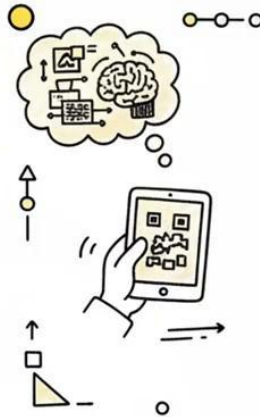
TLE: Business

Prospect Heights SD 23   6:236-AP1

Procedure for Requesting a Digital Resource

1) Staff follows the instructions HERE. **All programs should be reviewed with the building principal or department head first. Only after that should the program then be entered into Education Framework to begin the formal vetting process. All programs must support Board-approved curricula, be safe, and follow necessary data-privacy requirements.**

2) The Data Privacy Officer, who is the Director of Technology and Information Services, receives requests and audits the educational resource for privacy using Education Framework.
   a) 5 Stars (an IL-NDPA may not be required if no student data is used)
   b) 4.5 Stars (the IL-NDPA is Requested through Education Framework, an Exhibit E is signed on SDPC, or there is direct communication with the vendor)
   c) Less than 4.5 Stars (contact is made with the vendor to ameliorate the issues, if possible, and then a SOPPA agreement is finalized through an Exhibit E on SDPC or direct communication with the vendor)

3) With the score from Education Framework, the Data Privacy Officer gathers the approval team, which consists of the Technology Integration Specialist (TIS), Assistant Superintendent for Curriculum and Instruction, respective Principal, respective Instructional Coach, and the respective building representatives from the District Tech Connect technology committee. The need for the program is supported through a simple majority vote; however, the Data Privacy Officer and the Assistant Superintendent for Curriculum and Instruction have the final say if there are concerns about safety and/or cost. (See Appendix A for a copy of the rubric elements.)

4) The program in question is approved in Education Framework if there is either a score above 4.5 or the vendor makes the requested changes to be compliant with the privacy score. If the program is also approved by the approval team, then a countersigned vendor IL-NDPA is uploaded to the SDPC.

5) If the program request is denied by the approval team, the Data Privacy Officer responds to the request stating why the software application request was denied.

Our district has processes for vetting programs and services for student data privacy and security, and we regularly educate staff on the importance of, expectations for, and processes for such vetting. Our district ensures contract language and data-sharing agreements appropriately address student data privacy and security, and we have enforceable policies.

Data, Privacy, & AI
Student Safety

Google Accounts:
All Students K-8th
4th-8th Grade have Gmail, but they can only email teachers.

iPads:
1:1 for All Students K-8th
Classroom iPads for EC
Collected over all school Breaks

Clever:
App on the iPad that helps students login to other apps. Teachers also use Clever on both a laptop and an iPad, for login.
Help Link

CIPA- Children's Internet Protection Act (monitor online activities of minors, educate minors regarding appropriate online behavior, establish a safety policy, etc.) Filters/Blocking Internet access to inappropriate sites and images.

FERPA- Family Educational Rights and Privacy Act – protects the privacy of student education records. Provides parents right to inspect file, and make corrections.

COPPA- The Children's Online Privacy and Protection Act - a law dealing with how websites, apps, and other online operators collect data and personal information about kids under the age of 13.

SOPPA- Student Online Personal Protection Act - protecting student data collection by educational technology companies. Additionally, that is is used for educational purposes only.

- Know the formal steps for using/adopting any program, resource, or curriculum that collects student/staff data!
- Know the district's policies for adopting new apps, websites, technology and follow them, HERE!
  - Approved List of Apps and Sites, compliant with SOPPA.
- Choose the tech around which your team collaborates and plans.
  - We have access to a lot. Ask your mentor, instructional coach, Hannah, and/or principal! We likely have a program that fits your need!

TLE: Data Security
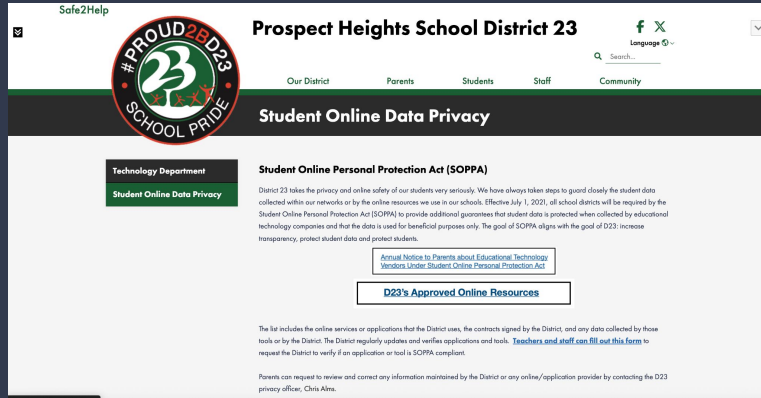
Our district website includes our data privacy and security policies and practices and is updated regularly. Our district has procedures for safeguarding data, and there are enforceable policies regarding where data is stored. Our district utilizes a documented, role-based process for permissions, has an incident response plan, and performs regular security audits.

PROTECTING STUDENT DATA IN D23

TYPES
Student data includes accounts for approved programs, use of iPad apps, and testing data

USES
Teachers use student data to modify instruction and give responsive, individualized feedback

SAFETY
Any program collecting student data **must** sign a data privacy agreement, which includes security measures and the educational-only uses of data

Important Data Privacy Laws
CIPA: monitors, enforces safety for, and educates on student internet use
COPPA: safeguards the data collected about kids under the age of 13
FERPA: protects the privacy of and grants parents rights to student education records
SOPPA: ensures third-parties use student data for educational purposes only

For more information, visit our "Student Online Data Privacy" page!

TLE: Professional Development

A SHARED DRIVE FOR SHARED DRIVES!

#PROUD2BD23 SCHOOL PRIDE

WHY?

→ **STUDENT PRIVACY:** LIMIT ACCESS TO STUDENT PERSONALLY IDENTIFIABLE INFORMATION (PII)

→ **ORGANIZATION:** ENSURE ROLES HAVE ACCESS TO TEAM/DEPARTMENT DOCUMENTS, WHICH WILL BE ORGANIZED WITHIN THE DRIVE

→ **EFFICIENCY:** PREVENT TIME NEEDED TO SHARE THINGS WITH TEAM MEMBERS

→ **ONBOARDING:** ALLOW FOR ACCESS FOR NEW MEMBERS OF A TEAM/DEPARTMENT

→ **GENERAL FYIS:** NOTHING WILL BE DELETED, JUST MOVED, AND WE WILL WORK ON THIS WELL THROUGH 24-25 SCHOOL YEAR. ALSO, IT IS ONLY TEAM/DEPARTMENT DOCS THAT NEED TO GO IN A SHARED DRIVE. ALSO, SEARCHING FOR A DOCUMENT WILL STILL BE THE EASIEST AND FASTEST WAY TO FIND IT!

Our district embeds privacy and security of student data into professional development for every role in every department. Our district provides accessible, relevant resources that include strong examples of best practices. All staff members participate in annual student data privacy training.

⏱ Expected course duration of 15 minutes · ⏳ Overdue by about 1 year

2024 Kevin Mitnick Security Awareness Training - 15 minutes

Start · 🌐 English (United States) ⌄

"Training Campaign - October 2024"

⏱ Expected course duration of 7 minutes · ⏳ Overdue by about 1 year

AI At Work: Use It Wisely

Start · 🌐 English (United States) ⌄

"Training Campaign - October 2024"

⏱ Expected course duration of 8 minutes · ⏳ Overdue by about 1 year

Double Trouble Trivia: Phishing Awareness Game

Start · 🌐 English (United States) ⌄

"Training Campaign - October 2024"

TLE: Classroom

Teachers implement a curriculum through our LMCs, specials, and general education classrooms; it promotes digital literacy, citizenship, and safety. Teachers are aware of and use the established vetting process for apps and programs, and teachers also model for and communicate to students and parents how data is collected and protected.

What's Next?

We will continue to apply for the remaining TLE seals. We are also actively working with the Student Data Privacy Consortium (SDPC) and the Learning Technology Center (LTC) for how our data-privacy agreements can be updated to account for A.I. use. This will be done through a best-practice lens with a data privacy and security mindset.