2025 NATIONAL STUDENT DATA PRIVACY REPORT

Part 2

CoSN TRUSTED LEARNING ENVIRONMENT PERSPECTIVES

CoSN

TRUSTED LEARNING ENVIRONMENT

Table of Contents

Introduction 2

Methodology Overview 3

Key Findings 6

The CoSN Trusted Learning Environment (TLE) Seal and District Privacy Performance 14

- **Leadership Practices** 14
- **Business Practices** 16
- **Data Security/Data Security Policy Management Practices** 17
- **Professional Development and Classroom Practices** 19

More from CoSN Trusted Learning Environment (TLE) Seal Recipients 22

Conclusion 28

Select CoSN Resources 30

Appendix A: The CoSN Trusted Learning Environment (TLE) Seal Program 31

- **CoSN TLE Seal Program Requirements** 32

Appendix B: About the Survey Respondents 36

Appendix C: Methodology 38

Special Thanks 43

About the Author 43

This research was funded by the Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect positions or policies of the Gates Foundation.

Introduction

In part 1 of the 2025 National Student Data Privacy Report from the Consortium for School Networking (CoSN), we provided results of a nationwide survey of school district privacy practices. The survey and subsequent report were designed to help us better understand the following:

- **Maturity of Privacy Practices:** How districts would assess the current state of their student data privacy programs.
- **Existing Supports:** The tools, resources, and systems currently available to help districts build and maintain student data privacy practices.
- **Additional Support Needs:** Types of further assistance or resources that districts would find most helpful.
- **Barriers to Improvement:** Challenges or obstacles that prevent districts from improving their student data privacy practices.

There was much to learn from those results, including information about challenges facing district ed tech leaders in improving student data privacy programs, resources needed, and steps that could be taken to help remove some of those barriers and build more in the way of district-wide scaffolding supports for the work. All of that and more is covered in part 1.

In addition, many of the CoSN Trusted Learning Environment (TLE) Seal recipients had participated in the survey. As such, we wanted to examine the reported level of maturity[1] of those TLE Seal recipient districts' student data privacy programs in comparison to those of other districts.

[1] Via applications for the CoSN TLE Seal program, CoSN also has the benefit of having reviewed the required student data privacy policies and procedures in place at CoSN TLE Seal recipient districts. Those requirements are provided in Appendix A.

We also wanted to understand how districts that reported they had achieved a certain level of maturity around their student data privacy programs had gotten there, in the hopes that their experiences might help others do the same.

This report examines the differences in the maturity of student data privacy programs across two sets of survey participants:

- Districts that have received the CoSN Trusted Learning Environment (TLE) Seal.
- Districts that have not yet received the CoSN TLE Seal ("non-TLE districts")[2].

This report also provides insights from district ed tech leaders about their student data privacy practices and how they have worked through some of common challenges uncovered in the research.

Methodology Overview

Between June 17, 2024 and Sept. 29, 2024, CoSN surveyed ed tech leaders about their district student data privacy practices. Respondents included CoSN members and non-members from school districts across the country.[3] We specifically wanted to gather information about district student data privacy programs, and not about district security programs. Although the two programs are related, and how personal information is protected is part of privacy, we wanted to focus specifically on the human-centered work of student data privacy.

[2] "Non-TLE districts" as the term is used in this report, is not intended to suggest or imply that those respondents applied for but did not achieve the TLE Seal. This is simply a term of convenience to indicate aggregated results from districts that are not currently TLE Seal recipients.

[3] 401 surveys were completed, and with consideration for the total number of school districts in the U.S., this represents a robust sample size; yielding +/- 4.90% maximum margin of error at the 95% confidence level.

Therefore, we defined privacy for respondents as "the decisions we make about what student personal information will be collected, how it will be used, where it will be shared, and how long it will be retained. This includes decisions about how to comply with applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), privacy provisions of other education laws, including Individuals with Disabilities Education Act (IDEA), National Student Lunch Act (NSLA), and more, including, for many districts, your state student data privacy law(s), as well as your district student data privacy policies."

Statistical segmentation was carried out as part of the analysis, dividing districts into distinct groups based on common characteristics across privacy performance and economics, with each group containing their own distinct performance characteristics.[4]

Census data from the 2020 American Community Survey (ACS) was integrated to capture the various demographic and economic indicators at the district level. (See Appendix C for specific variable sets integrated.)

The results of that portion of the survey are available in part 1 of the 2025 CoSN National Student Data Privacy Report.

For this report, we compared responses to survey questions that were specific to the CoSN TLE Seal requirements between districts that are CoSN TLE Seal recipients and non-TLE districts.

[4] Statistical segmentation is the process of dividing a large group of individuals into smaller, more manageable groups based on patterns in data. It uses statistical techniques to identify common characteristics within the data, helping to categorize districts for better understanding. This approach allows us to focus on unique traits that define each segment.

Specifically, survey respondents were asked to rate their district's performance against the 25 requirements of the CoSN TLE Seal program. These requirements are all centered around demonstrating that certain student data privacy policies, processes, and related practices are in place at the district. (See CoSN TLE Seal Program Requirements in Appendix A for details.)

Respondents were provided a rating scale of 1-4, with 1 being the lowest score, representing an absence of a particular practice at the district, and 4 being the highest score, representing a high level of maturity around a particular practice.

The aggregated results from survey respondents that are CoSN TLE Seal recipients - accounting for 77% of all CoSN TLE Seal recipients - were then compared with aggregated results of scores from survey participants that were non-TLE districts.[5]

We also interviewed a variety of ed tech leaders, including many who were instrumental in helping their district achieve the CoSN TLE Seal with the goal of learning more about how they were able to implement certain student data privacy practices within each of their districts. Those interviews serve as the source of district ed tech leader quotes within this report as well as the content in the section titled, More from CoSN Trusted Learning Environment (TLE) Seal Recipients.

Note that with respect to the results, percentages provided in this report have been rounded up, where applicable.

For additional information about the survey respondents, please refer to Appendix B.

[5] When assessing applications for the CoSN TLE Seal, CoSN also uses a scaled scoring rubric of 1-4 to indicate the maturity of a particular practice as demonstrated by evidence submitted by the applicant.

For additional information on the methodology, please refer to Appendix C.

Key Findings

When considering the survey responses:

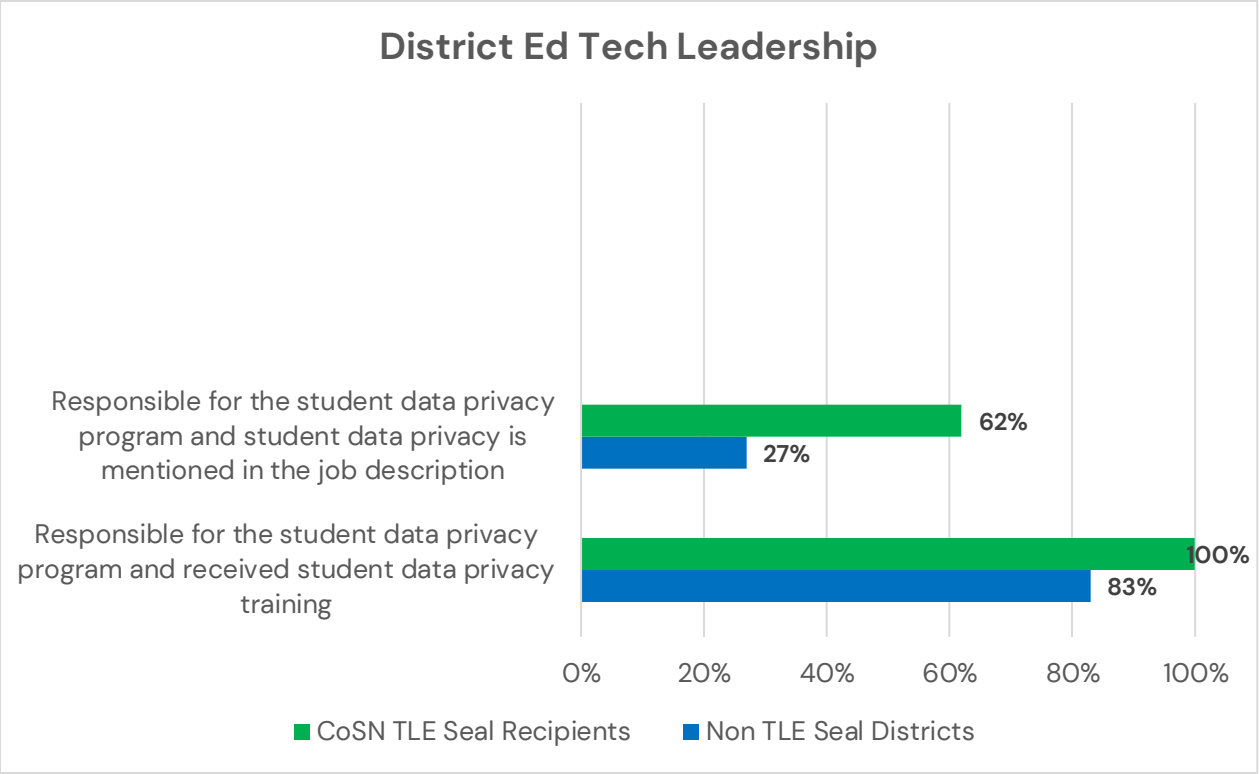
- Districts that have earned their CoSN TLE Seal or that have indicated that they are working toward obtaining one are far more likely to outperform other districts with respect to the overall breadth and maturity of their student data privacy programs.
- Districts that have not earned their CoSN TLE Seal and/or are not working toward earning a CoSN TLE Seal are significantly more likely to perform at a level that is below average with respect to the breadth and maturity of their student data privacy programs when compared to other survey respondents.

Ed Tech Leadership

We asked respondents who indicated that they were responsible for their district's student data privacy program whether that responsibility was referenced in their job description, whether they had received training in student data privacy, and how costs for the training were covered.

- Only 27% of non-TLE district survey respondents who reported that they were responsible for the district's student data privacy program reported that privacy was mentioned as a responsibility in their job description.
    - In contrast, 62% of TLE Seal recipients responsible for the student data privacy program reported that privacy was mentioned as a responsibility in their job description.

- 83% of non-TLE district survey respondents who reported that they were responsible for the district's student data privacy program reported having received student data privacy training, compared with 100% of respondents from CoSN TLE Seal recipient districts.



Employee and Vendor Management

Survey respondents who were CoSN TLE Seal recipients were more likely than non-TLE Seal districts to indicate that they were "extremely" or "very" concerned with ed tech vendor privacy and security practices; community service provider practices; and managing internal, employee practices.

However, CoSN TLE Seal recipients were *less* likely than districts that were not TLE Seal recipients to have similarly strong concerns with:

- Not being able to control the influx of free and reduced-cost classroom technologies brought in by teachers.
- Not being able to mandate privacy training for all employees.
- Lack of sufficient guidance on state laws.
- Inability to enforce internal, district-facing privacy policies.
- Lack of sufficient district policies to guide practices.

In part 1 of this report, we noted that the most frequently cited concerns fell into two dimensions.

1. Visibility and control over employees and vendors:

    - This includes the inability to manage employee privacy practices, as well as to understand ed tech vendor and community service provider privacy and security practices.

    Here, CoSN TLE Seal recipients and non-TLE Seal recipients share high levels of concerns with respect to the inability to manage employee behaviors and understanding the privacy and security practices of ed tech provider and community service organizations.

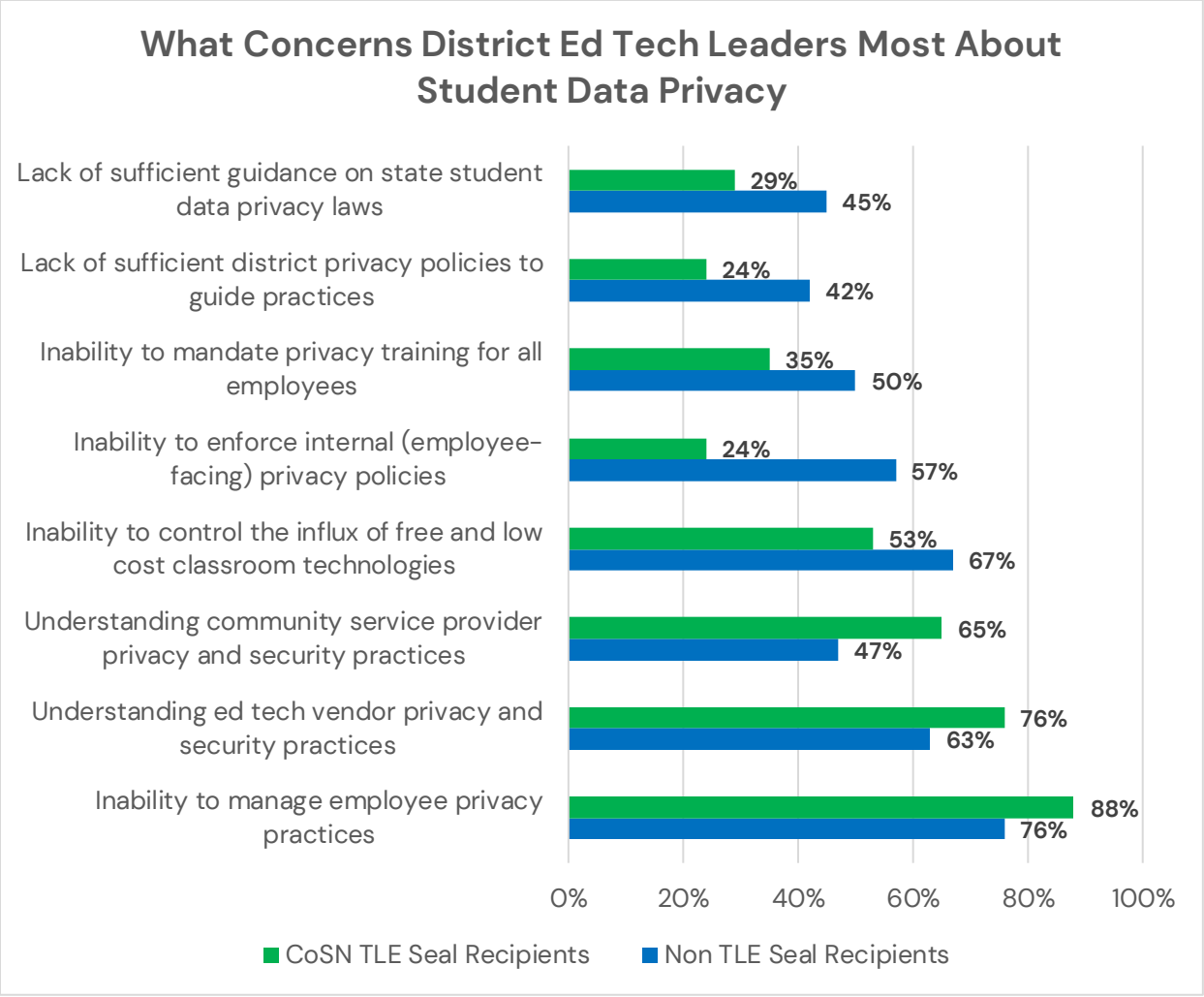
However, the second dimension of concerns tells a different story.

2. Lack of resources/support:

    - This includes the inability to enforce internal, employee facing privacy policies, contain the influx of free and low-cost classroom technologies brought in by teachers, and to mandate employee privacy training. It also includes a lack of sufficient district privacy policies to guide practices and a lack of sufficient guidance on state student data privacy laws.

With respect to resources and support, CoSN TLE Seal recipients appear to benefit from documented, enforceable policies at a level not experienced by non-TLE districts. The maturity of CoSN TLE Seal recipient districts' student data privacy programs is such that these districts have foundational practices in place which - while not eliminating concerns - lessen the degree to which these issues are the most pressing concerns.

We see similar trends for CoSN TLE Seal recipients around barriers to improving their student data privacy programs.



Barriers to Improvement

As noted in part 1 of this report, when we asked survey respondents questions about barriers to improving their districts' student data privacy programs, the most frequently mentioned barriers were time and manpower, each cited by 60% of respondents.

When looking at the barriers cited by CoSN TLE Seal recipients and non-TLE districts, all districts reported experiencing the same barriers, with a 1 to 15 point difference between the two sets of districts citing those barriers. The only exception to this was "expertise," which was cited as a barrier by 55% of CoSN TLE Seal recipients and 90% of non-TLE districts.

This stark difference between the two sets of districts in the number citing expertise as a barrier to improving the student data privacy program may be explained at least in part by the fact that - as noted above - all CoSN TLE Seal recipients who were responsible for the student data privacy program had been trained on student data privacy.

When looking at the *impact* of barriers on each group of districts, the differences between the two sets of districts become clearer.

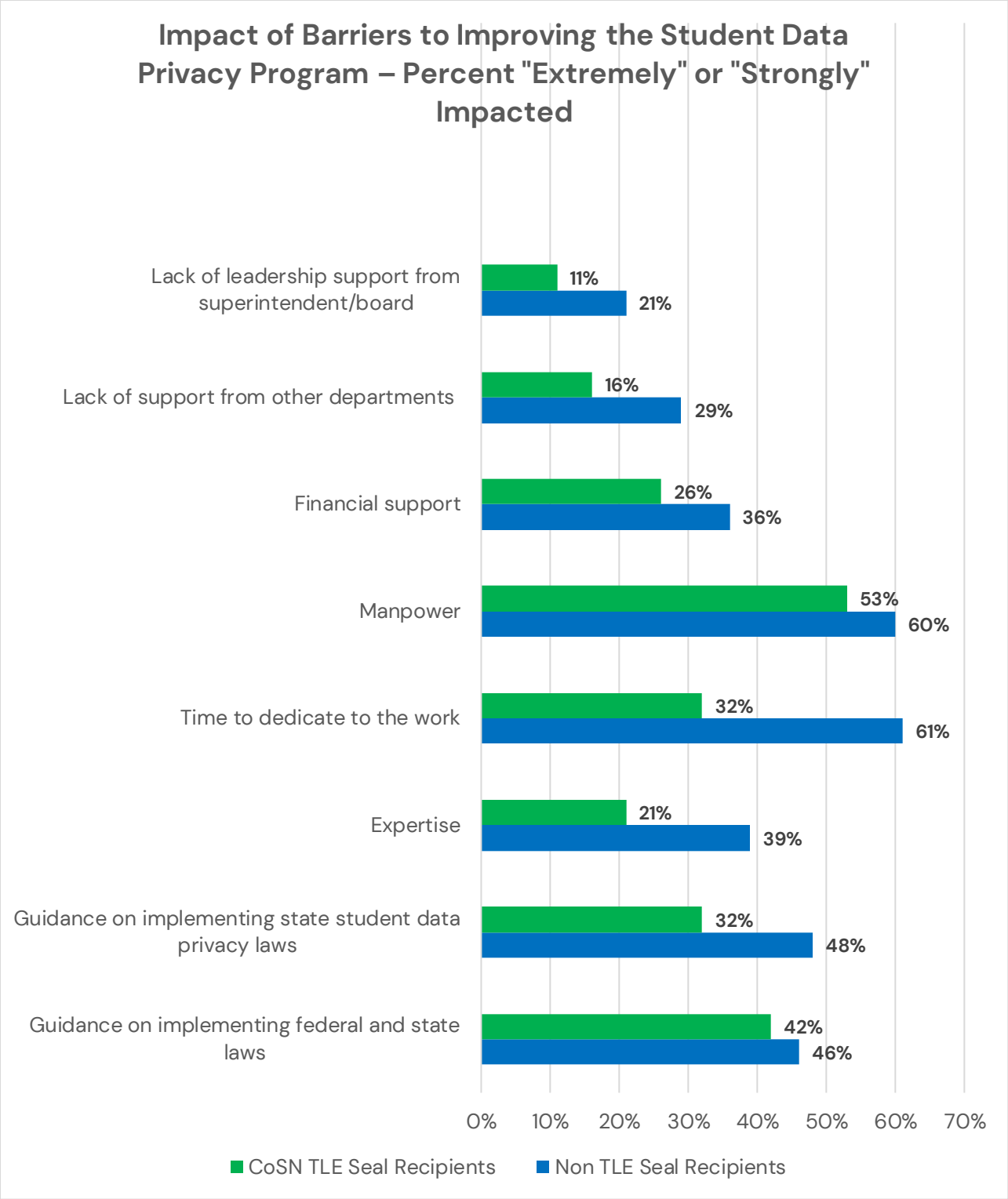
For example:

- 21% of non-TLE districts cited lack of support from their superintendent as an "extremely" or "strongly" impactful barrier to building and improving the student data privacy program.
    - Only 11% of CoSN TLE Seal recipients cited a lack of leadership support as an "extremely" or "strongly" impactful barrier.
- 29% of respondents cited a lack of support from other departments as an "extremely" or "strongly" impactful barrier to building and improving the student data privacy program.
    - Only 16% of CoSN TLE Seal recipients cited lack of support from other departments as being an "extremely" or "strongly" impactful barrier.

> *"It took me well over a year to convince my superintendent of the importance of the work. Then they left, and I'm starting all over again with the new superintendent."*
>
> *- District ed tech leader*

The largest differences in the impact of the barriers between the groups came with respect to expertise, cited as an "extremely" or "strongly" impactful barrier by 21% of CoSN TLE Seal recipients versus 39% of non-TLE districts, and time, cited by 32% versus 61%, respectively.

Note, however, that there is only a 7 point difference between the two sets of districts with respect to the impact of manpower as a barrier.


Impact of Barriers to Improving the Student Data Privacy Program – Percent "Extremely" or "Strongly" Impacted
Lack of leadership support from superintendent/board
11%
21%
Lack of support from other departments
16%
29%
Financial support
26%
36%
Manpower
53%
60%
Time to dedicate to the work
32%
61%
Expertise
21%
39%
Guidance on implementing state student data privacy laws
32%
48%
Guidance on implementing federal and state laws
42%
46%
0%
10%
20%
30%
40%
50%
60%
70%
CoSN TLE Seal Recipients
Non TLE Seal Recipients

Although time as a barrier has a very real impact on all districts, the smaller impact of time as a barrier for CoSN TLE Seal recipients may result from the fact that ed tech leaders in those districts have received training, have leadership more strongly primed to prioritize the work - including adequate resources for the work, and have been more successful at enlisting support from other departments. Certainly, the work becomes more efficient when ed tech leaders can spend their time doing the work, rather than getting buy-in to do the work.

The smaller impact of most barriers on CoSN TLE Seal recipients help to validate one of the key aims of the CoSN TLE Seal program, which is to help guide districts through creation and maturation of institution-wide student data privacy programs. To be effective at that work requires leadership support, a breakdown of departmental silos, and development of cross-functional supports to underpin the work. Overcoming or at least reducing the impact of barriers is a necessary in order to be able to improve.

"We started by establishing a Data Governance Committee. This involved identifying the roles within the district (that) should be a part of the committee, the purpose of the committee, and the scope of governance. After those were established, we developed a data governance policy that addressed governance over the following categories: regulatory compliance, risk management, data classification, systems and information control, (and) data transfer/exchange."

- Mike Van Vuren, deputy superintendent for CoSN TLE Seal recipient Bozeman School District #7 (MT)

The CoSN Trusted Learning Environment (TLE) Seal and District Privacy Performance

As noted above, as part of this work, we wanted to understand not just how districts were managing their student data privacy obligations, but also how the maturity of district privacy programs compared with the maturity of respondents that had earned the CoSN TLE Seal.

CoSN TLE Seal recipients outperformed non-TLE Seal recipients across all five of the required CoSN TLE Seal disciplines and across each of the requirements.[6]

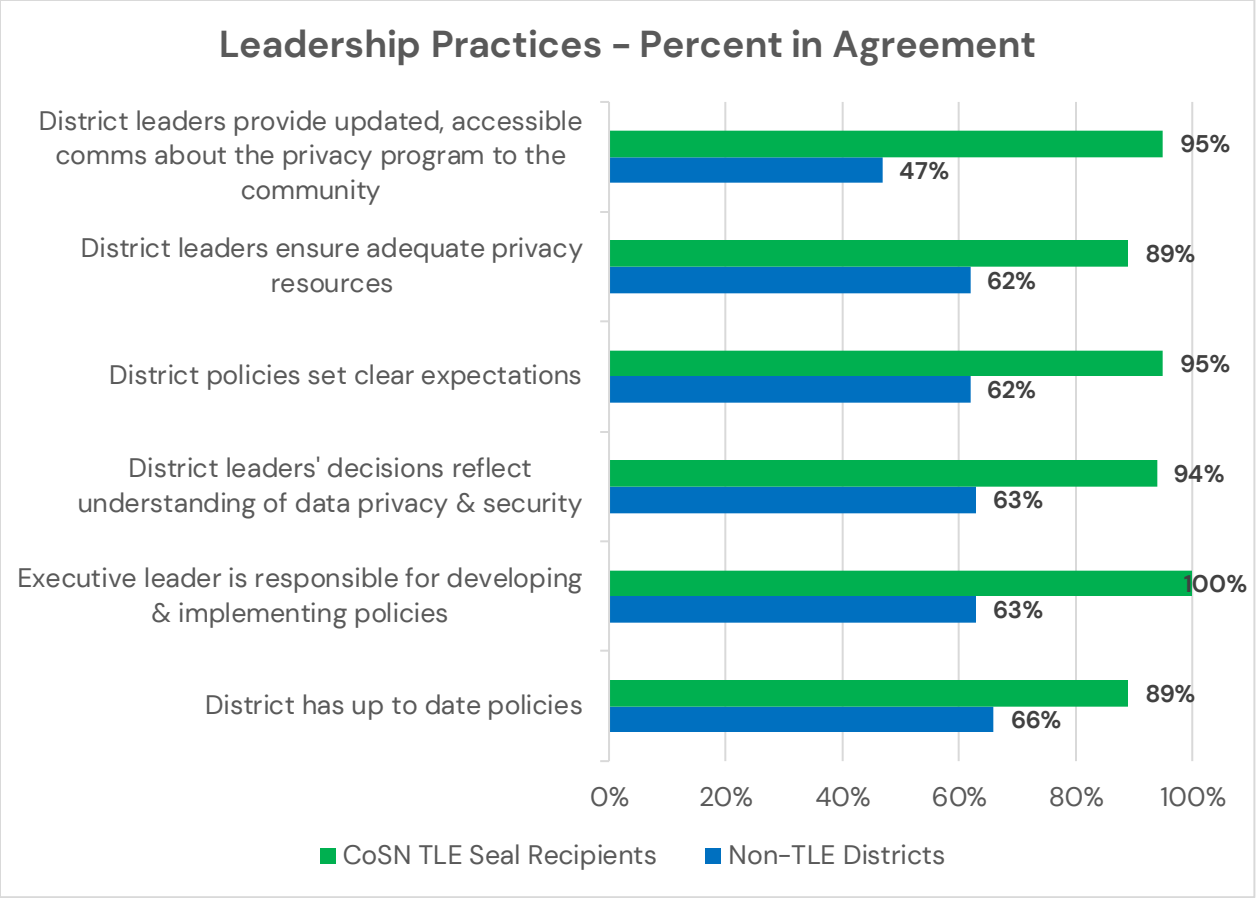
Those findings are provided below.

Leadership Practices

Across the Leadership Practices, CoSN TLE Seal recipients outperformed non-TLE Seal recipients in all areas. This is critical. District leadership drives the direction of the district, establishes the importance of the student data privacy program to all employees, provides the resources, and can establish or support the establishment and enforcement of policies.

As we saw in part 1 of the report, survey respondents typically gave their districts high marks for privacy leadership. However, those high marks did not always align with the presence of established, enforceable policies, training mandates, and removal of barriers to the work. As we'll see in several of the sections that follow, CoSN TLE Seal recipients prove to be the exception to that.

[6] As noted in part 1 of this report, we also found that TLE Seal recipients who participated in the survey were "High Performers," with respect to the maturity of their student data privacy programs.



"It's crucial for leadership to properly resource the data privacy function because it ensures that we continually have a clear understanding of our current data privacy landscape and can address any gaps proactively. By providing resources as needed, we ensure that all aspects of data privacy are considered, from legal compliance to technical security measures. This holistic approach helps protect our students' sensitive information from breaches and misuse, fostering trust among parents, students, and staff."

- Mike Van Vuren, deputy superintendent, CoSN TLE Seal recipient for Bozeman School District #7 in Bozeman, MT

Business Practices

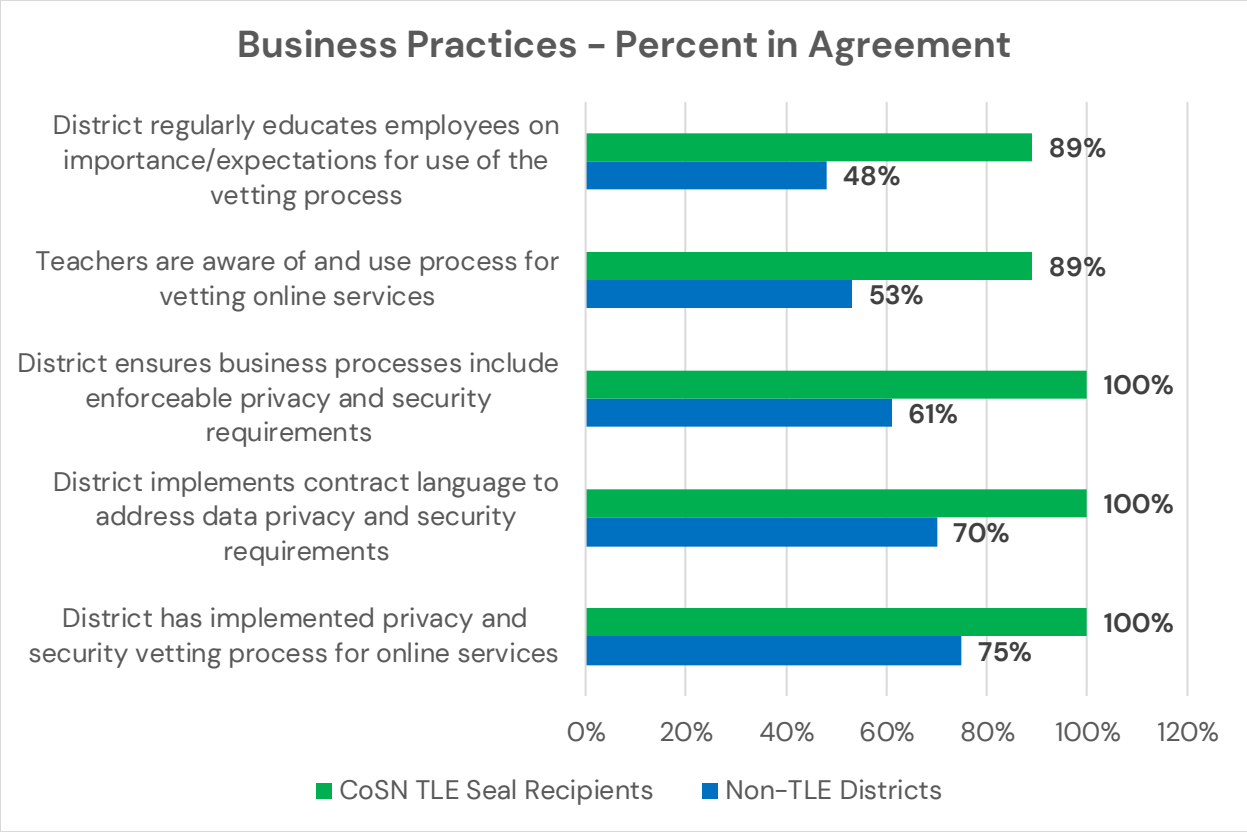
In practices that relate to their district assessment of and engagement with third-party online service providers, CoSN TLE Seal recipients again outscored the non-TLE districts. CoSN TLE Seal recipients all reported that they had developed and implemented a privacy and security vetting process for online providers and were implementing data protection agreements with those service providers.[7]

Importantly, CoSN TLE Seal recipients also report regularly training their employees about the vetting process, which may explain why they were less concerned than non-TLE districts with controlling the influx of free and reduced-cost technologies into the classroom (53% for CoSN TLE Seal recipients versus 67% for non-TLE districts).

CoSN TLE Seal recipients were also far less likely (24%) to be "extremely" or "very" concerned about an inability to enforce policies than non-TLE districts (57%), driving stronger overall compliance.

> *"For our vetting process, student data privacy is a top priority, strongly championed by our Chief Technology Officer (CTO). As a member of our administrative council, the CTO plays a key role in advocating for data privacy at both the administrative and board levels. This involvement has been instrumental in securing support from all key stakeholders for our technology initiatives."*
>
> *- Chris Davis, CCRE, cybersecurity specialist for CoSN TLE Seal recipient Deer Park Independent School District (TX)*

[7] When reviewing CoSN TLE applications, districts must provide evidence that the practices are in place as reported.



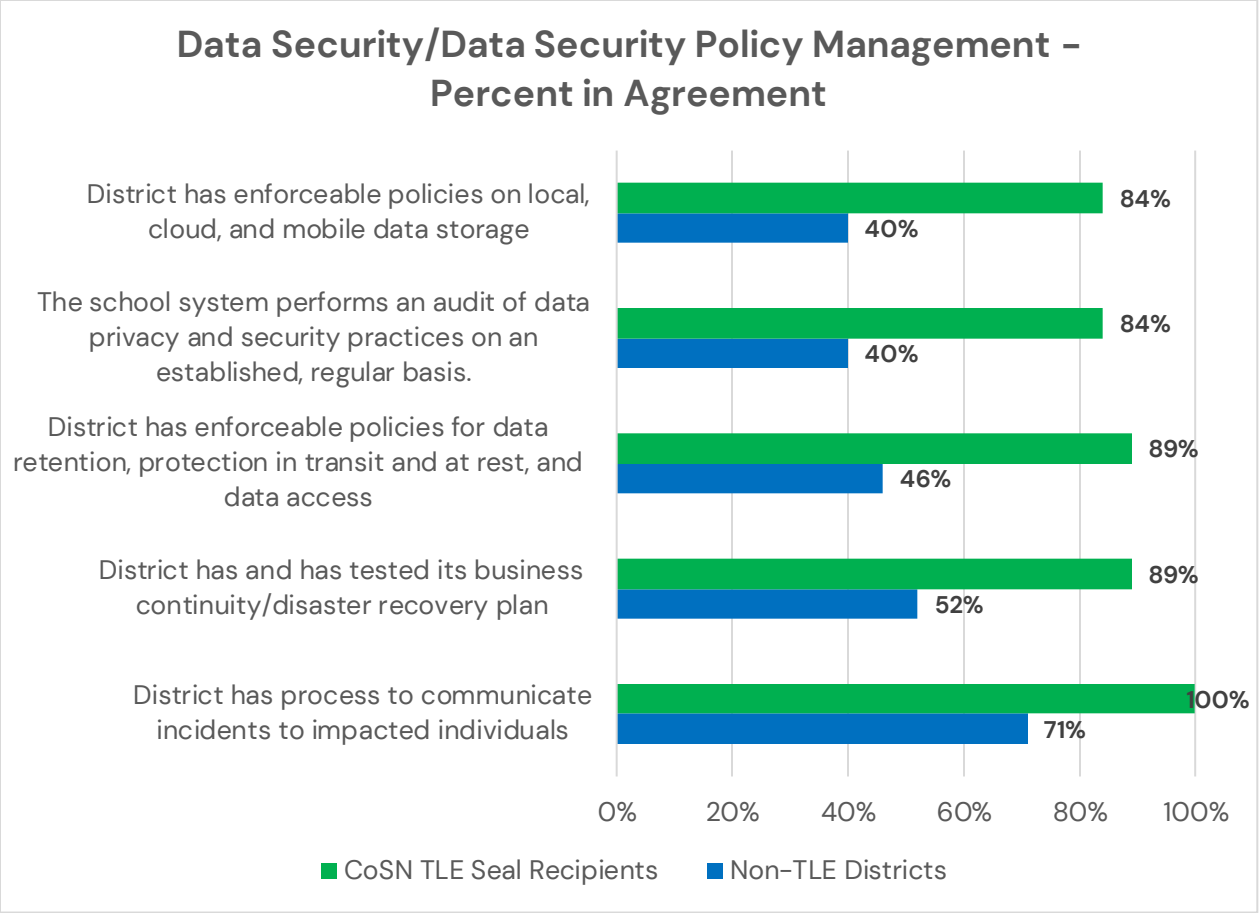
Data Security/Data Security Policy Management Practices

CoSN TLE Seal recipients seemed to far outpace non-TLE districts in their data security programs. Whether it is having enforceable policies to address certain security fundamentals; having a process to communicate data security incidents, having a verified, tested disaster recovery plan; or engaging in regular privacy and security program audits, CoSN TLE Seal recipients outperform non-TLE districts by nearly 2-to-1 in almost all practices included in the survey except one: 71% of non-TLE districts report having a plan in place to communicate data security incidents to impacted individuals.

We need not belabor the existing security gaps in school districts,[8] as that has already been widely reported. However, we will note that the absence of data security policies and practices - and controls supporting that work - should be a district priority.

> *"Ensuring a safe environment for students—both physical and digital—should be a priority for all school districts."*
>
> *- Chris Davis, CCRE, cybersecurity specialist for CoSN TLE Seal recipient*
> *Deer Park Independent School District (TX)*

[8] Homeland Threat Assessment 2024. U.S. Department of Homeland Security. Office of Intelligence and Analysis. "In recent years, ransomware incidents have become increasingly prevalent among US state, local, tribal, and territorial governments and critical infrastructure entities, disrupting services. K-12 school districts have been a near constant ransomware target due to school systems' IT budget constraints and lack of dedicated resources, as well as ransomware actors' success at extracting payment from some schools that are required to function within certain dates and hours."



Professional Development and Classroom Practices

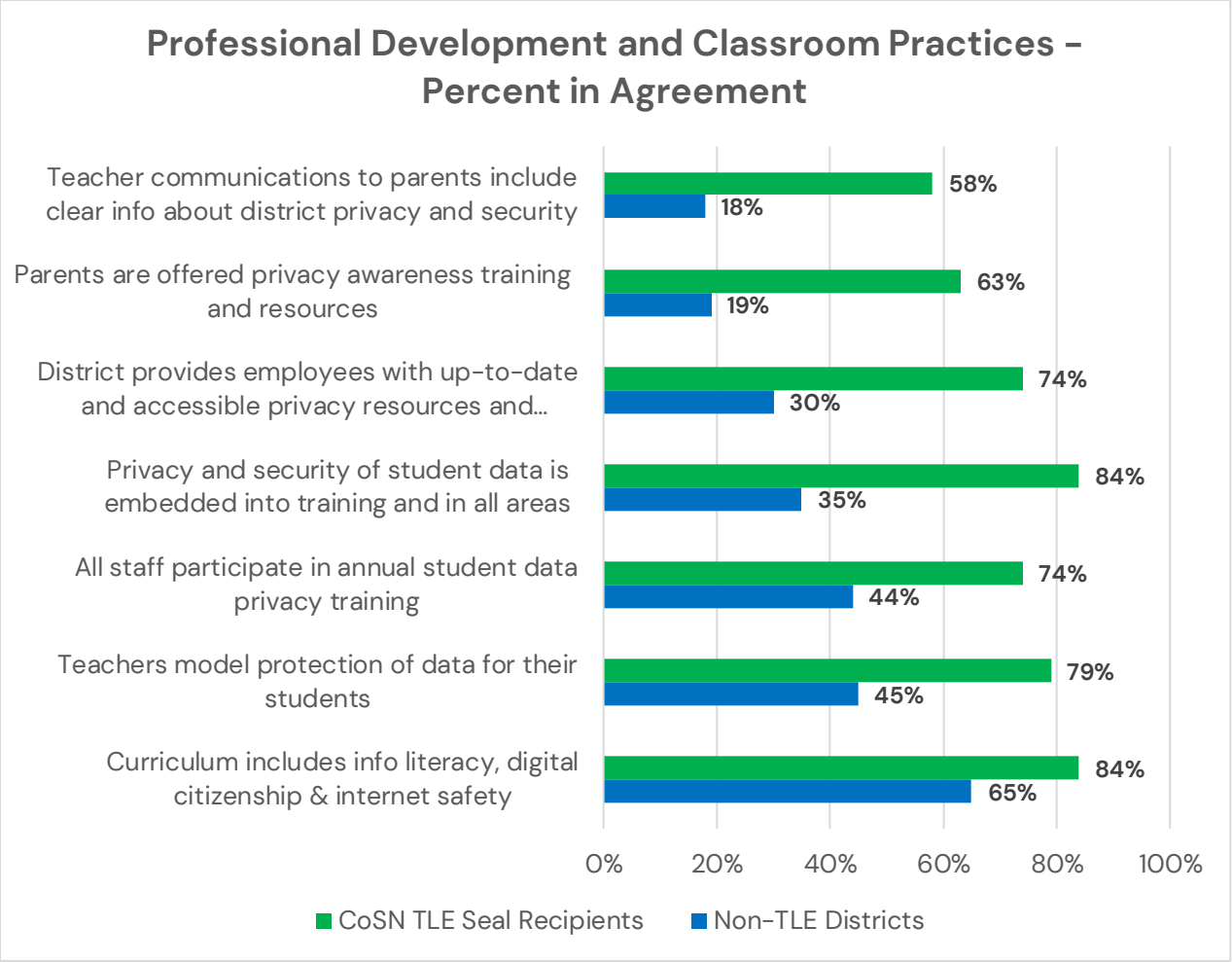
"We believe that every staff member - from the superintendent to bus drivers - may encounter student data in some capacity. Our goal is to ensure they are well-informed on how to handle and, more importantly, protect this sensitive information."

- Chris Davis, CCRE, cybersecurity specialist for CoSN TLE Seal Recipient Deer Park Independent School District (TX)

CoSN TLE Seal recipients also surpassed non-TLE districts in professional development and classroom practices. For example, when compared with non-TLE districts, CoSN TLE Seal recipients are:

- Over twice as likely to embed privacy and security training in all areas of professional development versus non-TLE districts.
- More than twice as likely to provide their employees with privacy resources, templates, and exemplars to follow.
- More than three times as likely to provide parents with privacy training and resources, supporting the district community within and outside the building walls.

This focus on implementing training, making privacy resources available to help reinforce the training, and transparency with the community are all required within the CoSN TLE Seal program to not only support improvements in student data privacy protections, but also to engender trust and support within the parent community for data privacy work.


Professional Development and Classroom Practices - Percent in Agreement
Teacher communications to parents include clear info about district privacy and security
58%
18%
Parents are offered privacy awareness training and resources
63%
19%
District provides employees with up-to-date and accessible privacy resources and...
74%
30%
Privacy and security of student data is embedded into training and in all areas
84%
35%
All staff participate in annual student data privacy training
74%
44%
Teachers model protection of data for their students
79%
45%
Curriculum includes info literacy, digital citizenship & internet safety
84%
65%
0%
20%
40%
60%
80%
100%
CoSN TLE Seal Recipients
Non-TLE Districts

More from CoSN Trusted Learning Environment (TLE) Seal Recipients[9]

We spoke with some of the district ed tech leaders who were instrumental in leading the work of achieving their district's CoSN TLE Seal. These profiles are provided to help further inform how some district ed tech leaders have approached the work, including how they have overcome some of the challenges.

Don Langenhorst, Ed.D., Technology Director for CoSN TLE Seal Recipient Dedham Public Schools in Dedham, Massachusetts

"We started by putting (data protection) contracts in place with our technology vendors. The process was just OK. But then I moved from thinking about it as a compliance exercise and instead thinking of it as more of an ethical issue. We realized that we had to go beyond the contract.

We adopted the structure of the TLE Seal program to get better at privacy and cybersecurity, with a goal of earning the seal. We took the CoSN TLE requirements, NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), and CIS (Center for Internet Security) requirements

> *"I think we have a moral responsibility to do better at protecting student privacy and cybersecurity."*
>
> *- Don Langenhorst, Ed.D., technology director for CoSN TLE Seal recipient Dedham Public Schools (MA)*

[9] Conversations have been condensed for this report.

and asked: 'What are we doing, what could we be doing, and what will we just never be able to do?'

In working through the TLE program, we built a data privacy team. We meet regularly and consider: 'What can we do next?' and 'How do we up our game?' Our disaster recovery work was a direct result of our data privacy team looking for ways to constantly improve. We leveraged resources from CoSN and others to get it done.

For privacy training, we do compete with other professional development priorities, but that's always getting better. We look at, 'What are the top priorities for our limited training time' and focus on that. We then supplement formal training with targeted newsletters.

We locked things down so teachers had to go through the technology vetting process, which also requires going through the curriculum team. When doing that or when implementing a change such as multi-factor authentication (MFA), we know we might get blowback and we need to first get leadership on board. Examples can be helpful in that conversation. You might say, 'Sure, MFA is a pain, but so is dealing with a hack.'

Teachers also learn about the process by talking to each other. When one teacher says to another, 'Maybe you can use that tech, but you have to check,' that tells us we're building a trusting relationship with staff. We really do try to say 'yes' wherever we can and solve for any gaps."

Bryan Drost, PhD, M.Ed, Executive Director for Educational Services for CoSN
TLE Seal Recipient Rocky River School District in Rocky River, Ohio

"Going through the pandemic, we had to restrict certain technologies for privacy concerns, and despite the training we had done, we realized the staff was just hearing us say 'no' and didn't understand the why behind it. We realized we needed to do more. For us, it's a process of constant education and reeducation. It comes down to awareness. We don't teach privacy in teacher ed, so we need to do it at the district.

> *"The staff training is so important. You don't know what not to do if you don't know even know what you're responsible for doing."*
>
> *- Bryan Drost, Ph.D., M.Ed., executive director for educational services for CoSN TLE Seal recipient Rocky River School District (OH)*

We were already really good about delivering a variety of training and we were able to slip privacy training into it. The Ohio education code requires training on FERPA as part of teacher licensure, so we leverage that to do more.

For example, we've really been able to emphasize that technology vendors' terms are a legally binding contract, and teachers in the state of Ohio don't have the authority to sign contracts for the district. With that understanding, we see everyone taking it more seriously. That's part of what the training has done for us. Staff begins to understand that this isn't the office of 'no.' This is just a function of our need to protect everyone when all is said and done.

Our technology vetting process was in place when I started with the district, and at the time, that had been put into board policy, which provides tremendous

weight. We also give our teachers frequent reminders of the process, including graphics with a flow chart.

Ultimately, what our staff wants from us is consistency and a willingness to listen and engage."

Thomas Molina, Chief Technology Information Security Officer for CoSN Trusted Learning Environment Seal Recipient Corpus Christi Independent School District in Corpus Christi, Texas

"When I arrived at the district, there was no formal program in place yet. However, when it came to privacy, we did have Texas law that made the district responsible for having such a program, and the mindset of upper management was in the right place at the right time to do the work.

One of the first things I recognized was the absence of documented policies and processes. So, I was able to tell management that I didn't need to start with a big financial investment to get things moving. Instead, I needed a year to work on policies and processes.

Part of how I was able to be effective was by leveraging my corporate expertise. I had been trained on how to sell and I used those concepts to put things into perspective in terms of pain points and solutions. For example, at the time, a pain point was that we didn't have cybersecurity insurance. To get it, we needed documented policies and processes, and we needed to teach security at every level in the district. That got me the go-ahead to do the work.

At one point, we were able to prevent a security incident from turning into a data breach. Afterwards I wrote up the report, and that's when eyes really opened. My superintendent really got it and paved the way for policy development, process development, and in-person training. We accommodated everyone's schedules to get it done, so that everyone - employees, parents, students - got some training.

"Key to the work is upper management being on board with your vision and trusting in your expertise."

- Thomas Molina, chief technology information security officer for CoSN Trusted Learning Environment Seal recipient Corpus Christi Independent School System (TX)

There was, of course, some pushback along the way, but we worked through it. It's all about managing change. It's natural for groups that communicate amongst themselves to think they're doing everything OK. They may perceive you as a threat if you try to suggest otherwise. You need to help people see that you're not the enemy - you're there to help them do their job better.

Policies and procedures are what holds you accountable over time, but to manage the change that comes along with that, I try to consider, 'Is what I'm doing augmenting the staff or does it just add more work to them?' We're always looking for ways to augment the staff, not create busy work.

"We need to consider not just the laws, but also how privacy impacts education. It's not a feature or an add-on."

- Thomas Molina, chief technology information security officer for CoSN Trusted Learning Environment Seal recipient Corpus Christi Independent School System (TX)

Part of what I do to keep learning is to partner with other districts. Working with yourself, you get nowhere. Working in groups provides tremendous value so I formed groups with other districts, which provides for exchanges of information. It allows us to be proactive, rather than reactive around the work."

Conclusion

CoSN TLE Seal recipients exhibit a level of maturity across a number of fundamental student data privacy practices that far surpasses that of most other districts. However, we know from our work with the CoSN TLE Seal recipient districts over the past several years that earning the CoSN TLE Seal did not come easily.

Most of the CoSN TLE Seal recipient districts did not necessarily start their path to the CoSN TLE Seal out with privacy programs that were stronger than those of any other districts. In fact, many ed tech leaders in CoSN TLE Seal recipient districts report having spent at least two years of work just to be in a position to have some confidence in applying. Even so, not all CoSN TLE Seal recipients earn the TLE Seal on their first application attempt.

As CoSN TLE Seal recipients make clear, persistence is a key ingredient to success, as are:

1. Recognizing that protecting privacy is a discipline of ongoing improvement. There is not - unfortunately - any way to guarantee that any data will ever be fully protected. What a strong privacy program requires is a commitment to an ongoing cycle of an examination of practices and a commitment to ongoing improvements.
2. Breaking down organizational silos. It is axiomatic that one simply cannot properly implement a district-wide student data privacy program without district-wide support, or close to it. Whether it's resourcing the privacy program, implementing privacy training, or building a privacy and security vetting program for online technologies, multiple teams within the district are implicated in the work. In addition, in many cases, the work requires

culture and behavioral changes, which - in any organization - is done most effectively when championed by leadership.

CoSN TLE Seal recipients inspire district leaders at all levels of their institutions to engage more fully in the work of building and improving student data privacy programs. They also stand as potential models for other districts looking for inspiration and guidance to improve their own student data privacy programs.

Select CoSN Resources

CoSN's Trusted Learning Environment State Partnership Program:

The CoSN Trusted Learning Environment State Partnership Program is designed to provide state education agencies with visibility into the overall breadth and maturity of district student data privacy programs across the state, along with resources to support common areas of challenge, district privacy training, and free TLE applications for all districts in the state. For more information, visit CoSN.org/TLEPartner.

CoSN's EmpowerEd Superintendent Initiative:

- Student Data Privacy. A School System Priority. An Essential Commitment
- The Role of Leadership in Protecting Student Data Privacy

CoSN Trusted Learning Environment (TLE) Seal Program Resources:

- CoSN Trusted Learning Environment Self-Assessment
- CoSN Trusted Learning Environment Examples of Evidence
- CoSN's Trusted Learning From the Ground Up: Fundamental Policies and Procedures Every District Should Have in Place

CoSN Student Data Privacy Initiative:

- CoSN Student Data Privacy Toolkit Part 1: Student Data Privacy Fundamentals
- CoSN Student Data Privacy Toolkit Part 2: Partnering with Service Providers
- CoSN Student Data Privacy Toolkit Part 3: Transparency and Trust

Appendix A

The CoSN Trusted Learning Environment (TLE) Seal Program

The CoSN Trusted Learning Environment (TLE) Seal program is a student data privacy rubric for school districts. It was developed by CoSN in partnership with district ed tech leaders from across the country, and with the partnership and support of AASA, the superintendent's association; ASBO, the school business official's association; and the nonprofit educational organization ASCD. The program requires that districts provide evidence demonstrating how they have implemented 25 student data privacy program practices, categorized into five disciplines:

- **Leadership**: Providing the guidance, frameworks and resources to direct the use and governance of student data in a manner that is transparent to all.
- **Business**: Establishing privacy and security vetting processes and implementing effective data protection agreements with technology providers receiving student data.
- **Data Security:** Implementing practices to protect the confidentiality of student data across all media and auditing regularly to maintain those practices over time.
- **Professional Development:** Requiring privacy and security training for all staff and offering related resources to all district community members.

- **Classroom:** Implementing educational processes and procedures to support transparency and build privacy knowledge while advancing curricular goals.

The evidence districts provide is assessed for completeness in meeting each requirement and for the level of maturity of the work. The CoSN TLE Seal indicates that the district has reached a certain level of maturity in their student data privacy program and is committed to ongoing improvements. It exists as a symbol of trust and transparency. Once earned, the CoSN TLE Seal is valid for two years, after which the recipient must demonstrate improvements in the student data privacy program in order to renew the TLE Seal.

Districts that apply for the CoSN TLE Seal receive feedback on how their application was scored, suggestions for improvements, recommendations on free guidance and related resources to inform the improvements, and a benchmarking report comparing their application scores to the aggregated scores of all CoSN TLE Seal recipients.

CoSN TLE Seal Program Requirements:

Leadership Practices:

- The deliberations and decisions of school system leaders reflect an understanding of data privacy and security.
- The school system has up-to-date policies and regulations addressing data privacy compliance requirements.
- The school system's policies and regulations set clear expectations for the protection of student data privacy and security, as well as the transparent use of data.

- A school system executive leader is identified as the person responsible for development and implementation of data privacy and security policies and practices.
- School system leaders provide transparent, updated, and accessible communications regarding the collection, management, and use of student data to their community.
- School system leaders ensure adequate resources are available to meet data privacy and security needs.

Business Practices:

- The school system has implemented a process for vetting online services for data privacy and security.
- The school system regularly educates its employees about the importance of, and expectations for, the use of the established vetting process for online services.
- The school system implements contract language and data-sharing agreements addressing student data privacy and data security.
- The school system ensures that all business processes associated with student data include enforceable data privacy and security requirements.

Data Security Practices:

- The school system website includes its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.
- The school system data privacy and security procedures include information about data retention periods for student records, data transmission technical protocols, data at-rest, and methods and controls limiting access to electronic data.

- The school system has enforceable policies regarding storage of data on local computers, mobile devices, storage devices, and cloud file-sharing and storage services.
- The school system utilizes a documented, role-based process when granting data and technology system access rights to educators, staff, and contractors.
- The school system has a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.
- The school system has a business continuity and disaster recovery plan that is verified and tested on an established, regular basis.
- The school system performs an audit of data privacy and security practices on an established, regular basis.

Professional Development Practices:

- Privacy and security of student data is embedded into training and professional development in all areas of school operations and academics.
- The school system provides employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.
- Parents are offered appropriate awareness training and resources about student data privacy and security.
- All staff members participate in annual student data privacy training related to applicable federal and/or state laws.

Classroom Practices:

- Teachers implement a curriculum to promote student information literacy, digital citizenship, and internet safety.

- Teachers are aware of and regularly use the school system's established process for vetting and procuring online services.
- Teachers model appropriate use and protection of student data for their students.
- Teacher communications to parents include clear information about the collection, use, and protection of student data.

Appendix B

About the Survey Respondents

Survey respondents came from 39 states and the District of Columbia.[10] They described their districts as follows:

Geographic distribution:

- 40% in rural areas.
- 38% in suburban areas.
- 14% in urban areas.
- The remainder spanned multiple geographic areas (e.g., rural and urban; rural and suburban; urban, rural, and suburban; etc.).[11]

District size by number of students:

- 4%: 50,000+ students.
- 21%: 10,000-49,999 students.
- 33%: 2,500-9,999 students.
- 26%: 1,000-2,499 students.
- 16%: less than 999 students.

District size by number of schools:

- 2%: 101-500 schools.
- 7%: 51-100 schools.

[10] CoSN did not receive survey responses from districts in the following states: Alaska, Delaware, Hawaii, Kansas, Kentucky, Louisiana, Mississippi, North Dakota, South Dakota, and West Virginia.

[11] National Center for Education Statistics (NCES) leverages geographic distribution based on urban, rural, suburban, and town, with further distinctions of large, midsize, and small, as well as fringe, distant, and remote for different areas. CoSN simplified to urban, rural, and suburban to avoid the overarching complexity for participants.

- 12%: 21-50 schools.
- 39%: 6-20 schools.
- 40%: less than 5 schools.

Free and reduced-price lunch percentage:[12]

- 19%: 81-100% free and reduced-price lunch percentage.
- 15%: 61-80% free and reduced-price lunch percentage.
- 25%: 41-60% free and reduced-price lunch percentage.
- 22%: 21-40% free and reduced-price lunch percentage.
- 19%: 0-20% free and reduced-price lunch percentage.

Survey participant data was analyzed in relation to performance as noted throughout the report.

[12] While free and reduced lunch percentage is often used as a stand-in for poverty rates, we have not used it as such in this report and provide it only in furtherance of participating district profiles.

Appendix C

Methodology

Between June 17, 2024 and Sept. 29, 2024, CoSN surveyed education technology leaders about their district privacy practices. We specifically wanted to gather information about district student data privacy programs, and not about their cybersecurity programs. Although the two programs are related, and how personal information is protected is part of the discipline of privacy, we were keen to focus on the human-centered work of student data privacy.

Therefore, we defined privacy for respondents as "the decisions we make about what student personal information will be collected, how it will be used, where it will be shared, and how long it will be retained. This includes decisions about how to comply with applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), privacy provisions of other education laws, including Individuals with Disabilities Education Act (IDEA), National Student Lunch Act (NSLA), and more, including, for many districts, your state student data privacy law(s), as well as your district student data privacy policies."

A total of 401 surveys were completed by education technology leaders, and with consideration for the number of districts in the US, this represents a robust sample size, yielding +/- 4.90% margin of error at the 95% confidence level.

In addition to survey questions specific to privacy practices, the survey also included questions on district characteristics, including location, number of students, grades supported, number of schools, and geographic regions.

For part 1 of this report, statistical segmentation was applied as part of the analysis, dividing district technology leaders (and their districts) into distinct groups based on common characteristics, each containing different dimensions.[13] Two core segments were then leveraged for the analysis:

1. **Privacy Performance Segments:** Privacy Protection Performance, Desire for Guidance, and Barriers to Improvements were used in combination to segment the audience into four distinct groups: 1) High Performers, 2) Above Average, 3) Average, and 4) Below Average.

2. **Economic Segments:** Economic segmentation was carried out by taking advantage of the fact that economic measures are correlated in populations: Areas with high unemployment and poverty tend to have low home values, and vice versa. Areas with high home values tend to have high employment and higher income levels. From these we examined 1) Top 3%, 2) Upper Middle, 3) Lower Middle, and 4) Bottom 12% in terms of economic performance of district areas.

The following population-level demographic variable sets from the U.S. Census Bureau 2020 American Community Survey (ACS) were integrated to capture the various demographic and economic indicators at the district level:

[13] Statistical segmentation is the process of dividing a large group of individuals into smaller, more manageable groups based on patterns in data. It uses statistical techniques to identify common characteristics within the data, helping to categorize districts for better understanding. This approach allows us to focus on unique traits that define each segment.

Variable Code	Description	Variable Code	Description
B01003_001	Total Population	B24011_006	Population in Computer, Engineering, and Science
B19013_001	Median Household Income	B03002_003	White alone, not Hispanic or Latino
B19301_001	Per Capita Income	B03002_004	Black or African American alone
B17001_002	Below Poverty Level	B03002_005	American Indian and Alaska Native alone
B23025_002	Employment Status	B03002_006	Asian alone
B23025_005	Unemployment Rate	B03002_007	Native Hawaiian and Other Pacific Islander alone
B25077_001	Median Home Value	B03002_008	Some other race alone
B25064_001	Median Gross Rent	B03002_009	Two or more races
B15003_022	Bachelor's Degree	B03002_012	Hispanic or Latino (of any race)
B15003_023	Master's Degree	B01002_001	Median Age
B15003_024	Professional School Degree	B28002_001	Total Households
B15003_025	Doctorate Degree	B28002_004	Households with Broadband Internet

For the analysis, dozens of variables from each of the following question sets were reduced to a smaller number of manageable dimensions using principal component analysis.[14]

1. **Privacy Protection Performance:** Twenty-four question battery reduced to 1) Leadership, 2) Business, 3) Security/Security Policy Management, and 4) Professional Development and Classroom.

[14] Principal component analysis, or PCA, is a statistical procedure that allows one to summarize the information contained in large data tables by means of a smaller set of "summary indices" that can be more easily visualized and analyzed.

2. **Privacy Protection Concerns:** Eight-question battery reduced to 1) Lack of Resources and 2) Visibility and Control over Vendors and Employees.

3. **Barriers to Privacy Protection:** Eight-question battery reduced to 1) Guidance and Expertise, 2) Resources, and 3) Support.

4. **Desire for Guidance:** Six-question battery reduced to a single dimension.

For this report, we compared responses to survey questions that were specific to the CoSN TLE Seal requirements between districts that are CoSN TLE Seal recipients and non-TLE districts.

Specifically, survey respondents were asked to rate their district's performance against the 25 requirements of the CoSN TLE Seal program. These requirements are all centered around demonstrating that certain student data privacy policies, processes, and related practices are in place at the district. (See CoSN TLE Seal Program requirements in Appendix A for details.)

Respondents were provided a rating scale of 1-4, with 1 being the lowest score, representing an absence of a particular practice at the district, and 4 being the highest score, representing a high level of maturity around a particular practice.

The aggregated results from survey respondents that are CoSN TLE Seal recipients - accounting for 73% of all CoSN TLE Seal recipients - were then compared with aggregated results of scores from survey participants that were non-TLE districts.[15]

[15] When assessing applications for the CoSN TLE Seal, CoSN also uses a scaled scoring rubric of 1-4 to indicate the maturity of a particular practice as demonstrated by evidence submitted by the applicant.

We also interviewed a variety of ed tech leaders, including many who were instrumental in helping their district achieve the CoSN TLE Seal with the goal of learning more about how they were able to implement certain student data privacy practices within each of their districts. Those interviews serve as the source of district ed tech leader quotes within this report as well as the content in the section titled, More from CoSN Trusted Learning Environment (TLE) Seal Recipients.

Note that with respect to the results, percentages provided in this report have been rounded up, where applicable.

Special Thanks

CoSN is deeply grateful to Aaron Hoffman and the team at Useful Research, Inc. for their invaluable assistance in analyzing the survey data for this report, including all of the principal component analysis (PCA) and segmentation analysis.

About the Author

Linnette Attai is project director for CoSN's Privacy and Trusted Learning Environment initiatives. As founder of the global privacy consulting firm PlayWell, LLC, Linnette provides strategic advice, training, policy development, and related guidance to a wide range of organizations. She is the author of an FTC-approved COPPA safe harbor program, and 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. She is a TEDx speaker and author of three books for school districts on protecting student data privacy.