CoSN
Leading Education Innovation

2025 NATIONAL STUDENT DATA PRIVACY REPORT

Part 1

Table of Contents

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

Student data privacy is at the forefront of education concerns nationwide. With over 130 state student data privacy laws enacted[1], and a steady stream of headlines about data breaches in schools, the stakes have never been higher. For school district technology leaders (referred to in this report as "district ed tech leaders"), safeguarding student personal information (referred to as simply, "student data")[2] has become a pressing challenge in an increasingly digital learning environment.[3]

Yet for all the news headlines and privacy laws, there hadn't yet been a systematic examination of how districts are building and maturing their student data privacy programs and the current state of those programs.

With that in mind, and with the idea that "what we can measure, we can improve," CoSN set out to measure student data privacy efforts. Specifically, we wanted to 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.

---

[1] National Association of Secondary Schools Principals, Top Issues In Education: Student Data Privacy.
[2] For this report, student data is defined as information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular student. The term should be read to be inclusive of student personal information, personally identifiable information, or any other information covered as such under federal and state student data privacy laws. We refer to this all as "student data" for convenience.
[3] The 2024 CoSN State of EdTech District Leadership Report illustrated that student privacy is a critical priority for ed tech leaders.

- **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.

While there is still more to learn about how districts are attending to the protection of student data than we were able to capture in the survey and subsequently in this report, we are able to provide a look at the state of student data privacy programs within districts in a way that has not previously been considered.

Importantly, the survey results as detailed in this report also provide us with valuable insights into what we may need to do to better help districts improve their privacy practices, as told to us directly from those responsible for doing just that.

It is our intention that this report be leveraged to remind education institutions and the broader education ecosystem – including legislators, state education agencies, parents, and other community members – that what districts need is not a critique of their work but guidance and support.

Methodology Snapshot

Between June 17, 2024 and Sept. 29, 2024, CoSN surveyed district ed tech leaders from across the country about their district student data privacy practices. We specifically wanted to gather information about privacy programs, and not about security programs. (While data privacy and security are closely related and while there is overlap between the two, they are in fact two distinct disciplines that must operate in partnership to properly protect student data.)

The survey included 56 questions about each participant's district; their privacy training and expertise; the maturity of specific, foundational privacy practices; resource needs; and barriers to improvements.

Census data were integrated from the 2020 American Community Survey (ACS) to capture demographic and economic indicators at the district level.

For details on the methodology, including the analysis methods, please see Methodology Overview and Appendix C.

To that end, in addition to providing the survey results, we've developed a companion report[4] providing insights directly from district ed tech leaders about how they have worked through some of the common challenges uncovered in the research. We have also provided references to CoSN resources that are designed to educate districts on certain student data privacy practices and guide them on development and implementation of those practices at their districts.

There are many other organizations in the ecosystem that provide districts with valuable resources to support various aspects of student data privacy. It is our hope that this report will not only highlight existing needs, but also inspire the creation of additional tools and supports to help districts continue to strengthen their student data privacy protections.

Finally, it's important to recognize that while this report focuses solely on student data privacy, districts are also responsible for safeguarding the privacy of parent and employee personal information under their care.

Key Findings

CoSN's 2025 National Student Data Privacy Survey Report provides results of a survey of district ed tech leadership focused on the state of student data privacy protections in place at school districts across the country. The results revealed information about the scope and maturity of student data privacy programs, as well

[4] See Part 2: 2025 CoSN National Student Data Privacy Report: CoSN Trusted Learning Environment Perspectives.

as specific barriers to improvement and the resources needed to help districts overcome those barriers and drive improvements in the work.

The results illustrate that while district ed tech leaders are committed to the work, many districts are still struggling to put a number of foundational student data privacy practices in place and execute a student data privacy program that encompasses what would be considered fundamental requirements for any privacy program.

Gaps include an absence of job descriptions for those responsible for building and implementing the student data privacy program that mention privacy responsibilities, a lack of basic privacy policies and student data privacy training, and a reported inability to enforce district privacy policies and manage employee behavior to better protect student data privacy.

In practice, this may reflect a lack of district leadership emphasis on the importance of the work across two dimensions:

1. Providing signals that the work of protecting student data privacy is critical, such as by providing job descriptions for employees responsible for building, implementing, and improving the student data privacy program that address those requirements as a core component of the role, communicating to all employees the importance of fully participating in the work, and modeling strong privacy behaviors for staff.
2. Taking tangible steps to remove barriers to provide the needed privacy training, create or allow for the creation of needed policies, and develop and implement reasonable and responsible policy enforcement mechanisms.

Specific findings include the following:

Ed Tech Leadership

- 73% of those who reported that they were responsible for the district's student data privacy program noted that privacy was *not* mentioned as a responsibility in their job description.
- 17% of those who reported that they were responsible for their district's student data privacy program also reported that they had not received *any* training on student data privacy.
    - 25% of those who were responsible for student data privacy in their district and had received privacy training had to personally cover the costs of that training.

Employee and Vendor Management

- Employee-related concerns were extremely or very concerning to 89% of respondents.
    - 76% were "extremely" or "very" concerned about an inability to manage employee behavior.
    - 69% were "extremely" or "very" concerned about an inability to control the influx of free and low-cost classroom technologies.
    - 55% were "extremely" or "very" concerned about an inability to enforce internal, employee-facing privacy policies.
    - 49% were "extremely" or "very" concerned about an inability to mandate employee privacy training.
- Insufficient privacy and security policies and district policy mandates were "extremely" or "very" concerning to 58% of respondents.

- 63% were "extremely" or "very" concerned about understanding ed tech vendor privacy and security practices, but only 43% were similarly concerned with community service provider privacy practices.

District Student Data Privacy Performance

- District ed tech leaders were generally hampered by a lack of certain foundational privacy and security policies at their districts, the inability to enforce internal policies and processes, including technology vetting processes, and the inability to implement privacy training for all employees.
- **Districts that have earned their CoSN Trusted Learning Environment (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 breadth and maturity of their student data privacy programs.**[5] (See Appendix D for more information about the CoSN Trusted Learning Environment (TLE) Seal program.)

Districts that have not earned their CoSN TLE Seal and/or are not working on 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.

[5] For more information about how CoSN TLE Seal recipient responses compare with districts that have not earned their CoSN TLE Seal, see Part 2: 2025 CoSN National Student Data Privacy Report: CoSN Trusted Learning Environment Perspectives.

- These below-average districts did not typically have sufficient support from leadership and other departments for building and improving their student data privacy programs.

Barriers to Improving Student Data Privacy Practices

- 60% of respondents noted that time and manpower were barriers to improvement.
- A need for guidance on federal laws (47%), state laws (46%), and privacy expertise generally (38%) were more frequently cited as barriers than financial resources, which was cited by 36% of respondents.
- 20% of respondents cited lack of support from their superintendent as a barrier to the work.
- 28% cited a lack of support from other departments as a barrier to the work.

Requests for Guidance

- Respondents indicated (at levels of between 62% to 82%) that all of the following would be helpful: guidance on implementing federal and state privacy laws, policy templates provided by states, guidance on implementing specific privacy practice requirements, training, and help prioritizing the work with the superintendent.

Opportunities for Improvement

Overall, the findings suggest that while district ed tech leaders are committed to the work, the organizational scaffolding needed to develop, implement, and maintain a student data privacy program may not yet be in place across districts. The results indicate that the following would be key to improvements:

- Renewed leadership focus on student privacy as a core priority, including elevation of importance of student data privacy work and a keen focus on

fundamental privacy and security policy development, policy enforcement, mandatory privacy training for all employees, and transparency about the privacy work with district community members. These measures would all meaningfully impact and improve the state of student data privacy practices.

- Support for district ed tech leaders in the form of training and implementation guidance would also meaningfully impact district student data privacy program performance.

All of the above findings are discussed in further detail below.

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.[6] 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.

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

[6] 401 surveys were completed, and with consideration for the total number of school districts in the US, this represents a robust sample size; yielding +/- 4.90% maximum margin of error at the 95% confidence level.

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.[7]

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.)

In addition, for Part 2 - 2025 CoSN National Student Data Privacy Report: Trusted Learning Environment Perspectives, we compared responses from districts that were CoSN Trusted Learning Environment (TLE) Seal recipients with districts that were not to consider and to illustrate differences in the results.

We also interviewed a variety of ed tech leaders from districts that are CoSN TLE Seal recipients to learn more about how they were able to implement certain student data privacy practices within each of their districts. Edited versions of those interviews and other quotes from those ed tech leaders are also included in Part 2.

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

[7] 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.

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

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

Detailed Findings

Student Data Privacy Expertise

Responsibility for student data privacy in school districts typically falls under the purview of the technology department, and 89% of respondents reported that they were responsible for the student data privacy program in their district. Of those, the four most commonly reported titles were:

- Director of Technology
- Chief Technology Officer
- Director of Information Systems
- Chief Information Officer

A full 78% of those who reported that they were responsible for the district's student data privacy program reported that privacy was not mentioned as a responsibility in their job description.

In addition, 16% of those who reported that they were responsible for the student data privacy program in their district also reported that they had not received any training on student data privacy.

For those who did report having received privacy training, the vast majority (79%) reported that the training was either free or that the costs were covered by the district or the state. Of the remaining group that reported having to personally pay for training, 25% reported that they paid for all of it - this despite the fact that privacy qualification requirements and/or responsibilities were absent from their job description.

Bear in mind that technology, privacy, and security are separate disciplines, each requiring special expertise. Thus, an individual who applied for a job as a technology or information officer would not necessarily have - nor would they expect to be required to

have - privacy or security expertise if it was not listed as a required job responsibility and qualification.

Further, the lack of reference to such a large and critically important responsibility as developing and maintaining a student data privacy program to support the district's compliance with applicable federal and state student data privacy laws, would seem to warrant an appropriate measure of reference and emphasis in the job description.

In a similar fashion, in the absence of pre-qualification requirements, privacy training - including training on applicable privacy laws and on how to build a privacy program - should be provided to those responsible for the work without the need to incur any personal cost.

Prioritizing Student Data Privacy

Despite a lack of employer-provided training or codification of the work of building and improving a student data privacy program as part of a formal job description, respondents clearly prioritized the work. When asked, "Where does protecting student data privacy rank in terms of your priorities," 88% ranked it as one of their top two priorities, with 46% ranking it as their top priority. This aligns with findings from CoSN's 2024 State of Ed Tech Leadership Report, as referenced above, which showed that cybersecurity and privacy are the top two priorities of district ed tech leaders.

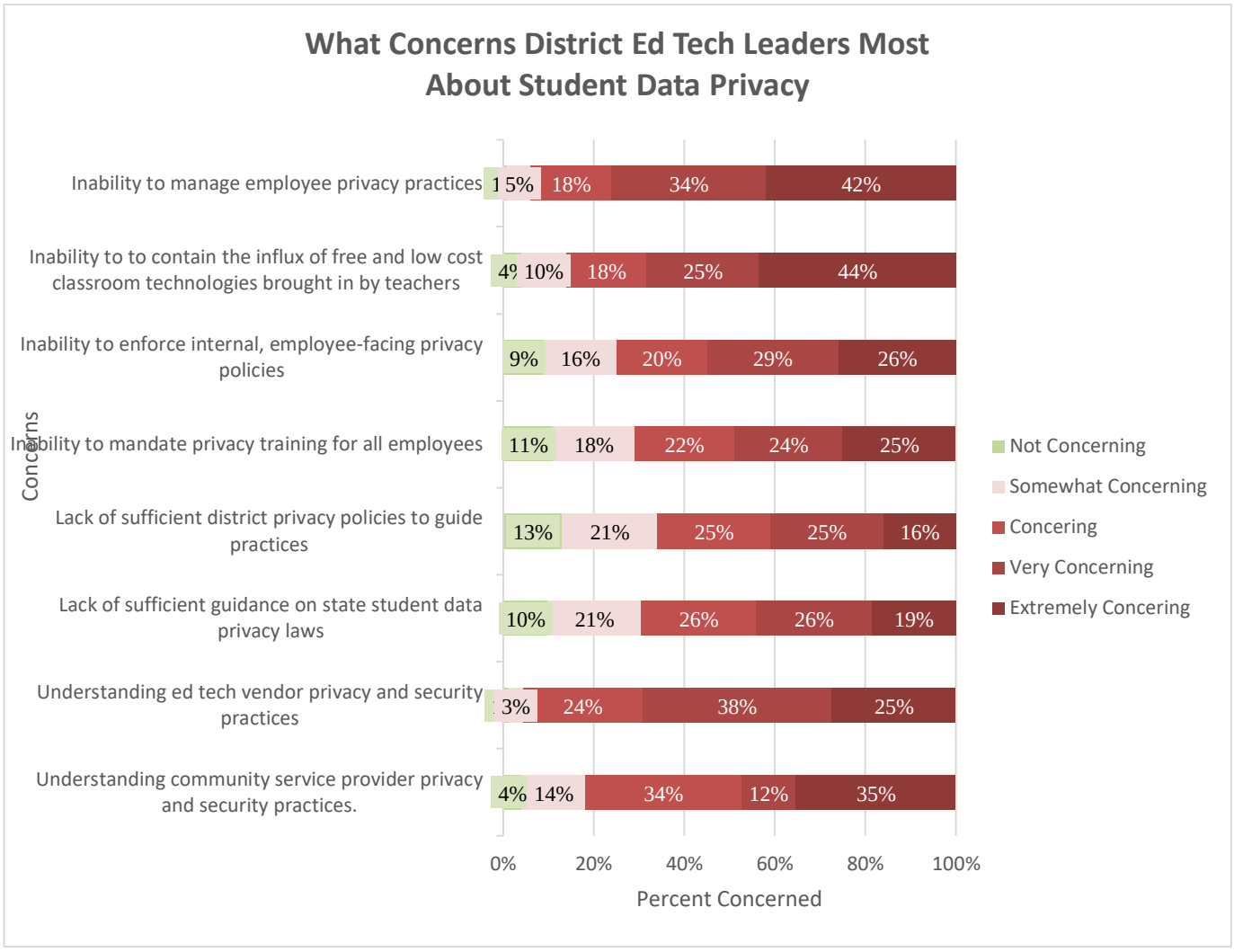
District Ed Tech Leaders' Privacy Concerns

When asked what, specifically, concerned district ed tech leaders most when it comes to protecting student data privacy, the results showed a clear focus on internal practices. *This is critically important*, as the privacy of student data can't be properly managed - including when shared externally with technology providers and community service organizations - without first establishing internal rules for what student data may be collected and shared, how it may be used, and how it must be protected.

It is those internal determinations, codified in policy that - when applied externally - help to ensure adequate and consistent privacy protections for the data in alignment with each district's consideration for applicable laws and district policies.

Specifically, with respect to district leadership-related practices:

- Employee-related concerns are extremely or very concerning to 89% of respondents.
    - 76% were "extremely" or "very" concerned about an inability to manage employee privacy practices.
    - 69% were "extremely" or "very" concerned about an inability to contain the influx of free and low-cost classroom technologies brought in by teachers.
    - 55% were "extremely" or "very" concerned about an inability to enforce internal, employee-facing privacy policies.
    - 49% were "extremely" or "very" concerned about an inability to mandate employee privacy training.
    - 41% were "extremely" or "very" concerned about a lack of sufficient district privacy policies to guide practices.



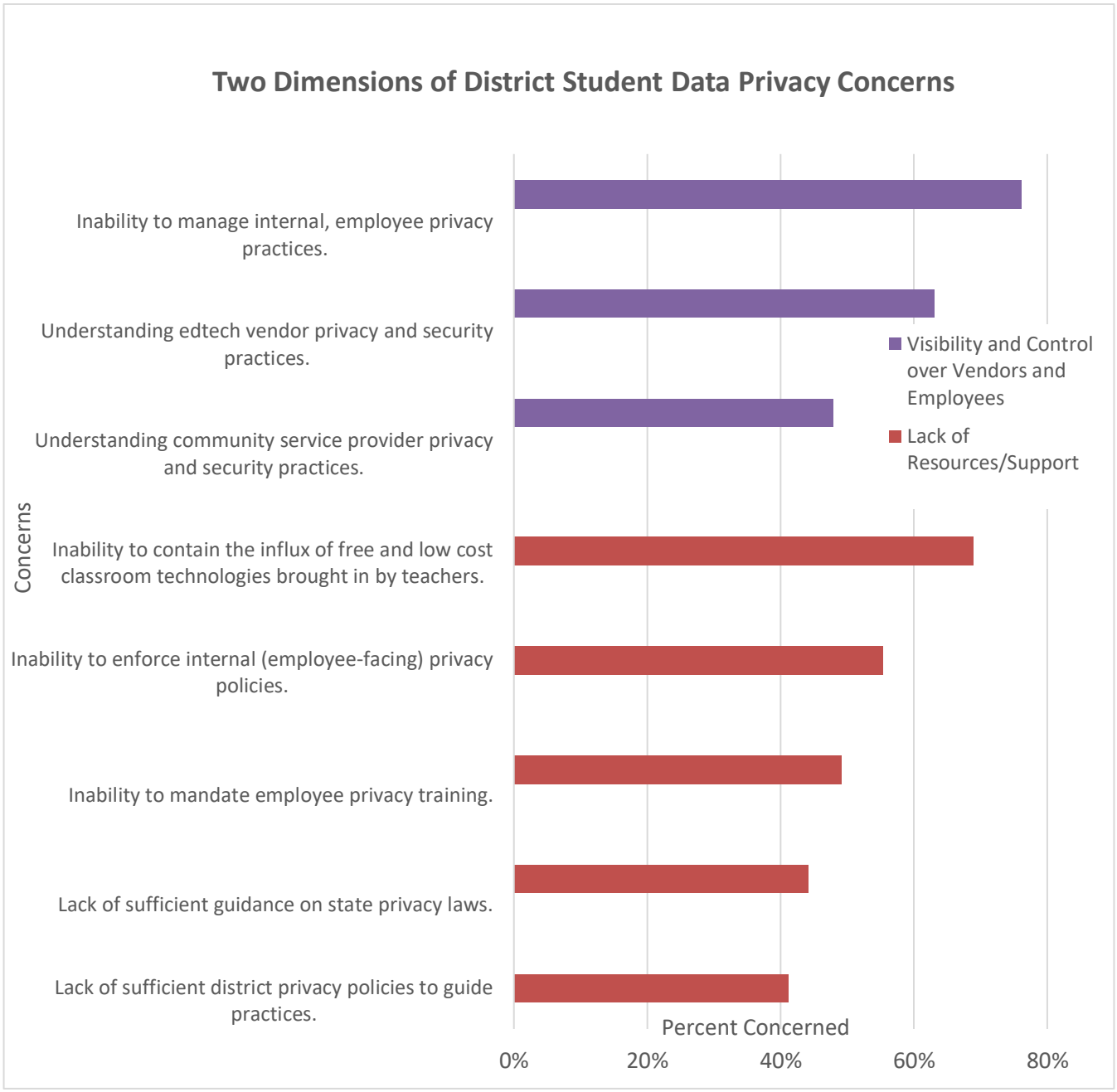
It's noteworthy that, as illustrated in the chart above, the majority of respondents indicated that they were "extremely" or "very" concerned with an inability to manage employee privacy practices, including not being able to manage the influx of free and low-cost technologies into the classroom. This is another crucial point to understand. Although the ed tech leader may be responsible for developing and implementing a student data privacy program, such a program can only be effective if *all* employees understand the importance of the work and follow established policies, procedures, and guidance.

In short, a privacy program cannot be successful if employees aren't informed of, aware of, and adhering to policy and process requirements, which is not possible in the absence of enforceable policies and training to help guide their behavior.

Analyzing the data further, we note that the most frequently cited concerns fall into two dimensions:

- 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.
- 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 mandate privacy training for employees. Also of concern was a lack of sufficient district privacy policies to guide practices and a lack of sufficient guidance on state student data privacy laws.

Both dimensions need to be considered in order to create a more complete view of the concerns ed tech leaders have around student data privacy protection.



When considering solutions to these issues, unfortunately, ed tech leaders do not typically have supervisory or other authority over employees outside of the technology department. Thus, they are not able to mandate that employees follow policies or otherwise comply with district privacy program requirements.

Instead, as is typical in most organizations, both within and outside of education, leadership - in this case, the superintendent - is responsible for establishing for all

employees the importance of protecting student data, leveraging guidance from technology leadership to establish adequate policies for the student data privacy program, ensuring that those policies are enforced, and providing technology leadership with the agency within the institution to do the work.

Of course, superintendents are faced with a matrix of priorities, so bringing a superintendent on board as a champion of student data privacy work can sometimes be a time-consuming exercise. In fact, when asked what sort of guidance might be helpful, 62% of respondents cited, "help prioritizing the work with my superintendent."

***

Looking at external factors, 63% were "extremely" or "very" concerned about understanding technology vendor privacy and security practices, but only 43% were similarly concerned with community service provider privacy practices. This is noteworthy when we consider that community service providers - organizations that are affiliated with or operate independently from the districts and that may provide educational, social, and related supports - often have access to very sensitive information related to a variety of student needs.

Attending to both employee and vendor practices, and providing ed tech leaders with the agency and resources needed to properly implement student data privacy programs are necessary for success.

Assessing Student Data Privacy Practices

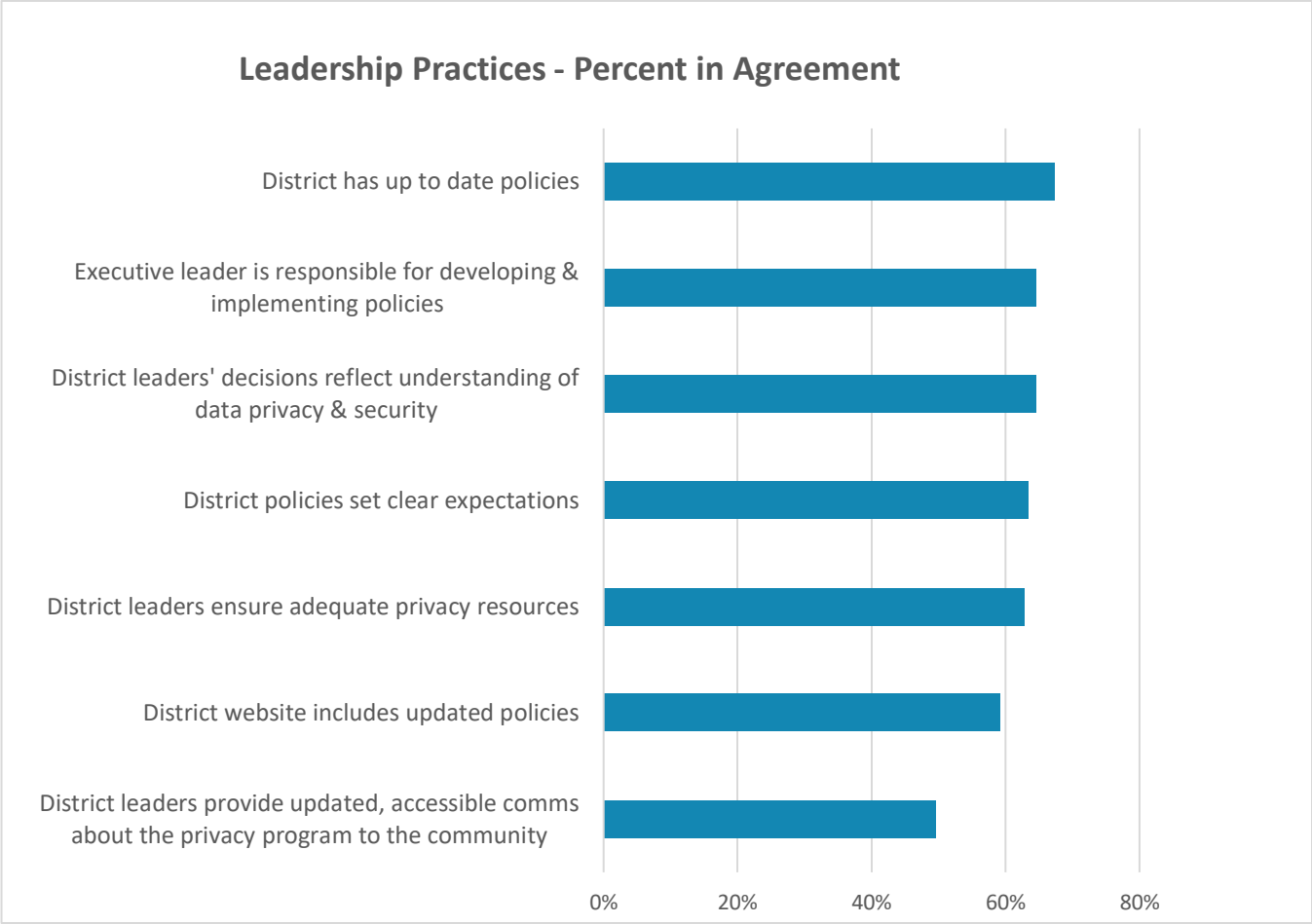
A core section of the survey involved asking participants to assess their districts around a set of foundational privacy practices sourced from the CoSN Trusted Learning Environment (TLE) Seal Program.[8]

For the data analysis, we collapsed the requirements into four disciplines that align with the CoSN TLE Seal Program requirements. Those results are shared in the pages that follow.

Leadership Practices

Standing somewhat in contrast with other findings discussed in this report, survey participants were generally complimentary about their leadership, with the majority indicating that the district had up-to-date policies to govern privacy practices, and that leadership demonstrated a clear understanding of data privacy and security requirements, ensured adequate resources were in place to support the student data privacy program, and - as noted in the last two lines in the chart below - ensured that district policies and other clear, accessible communications regarding the district's student data privacy program were readily available to community members.

[8] For information about the CoSN Trusted Learning Environment (TLE) Seal Program, see Appendix D.



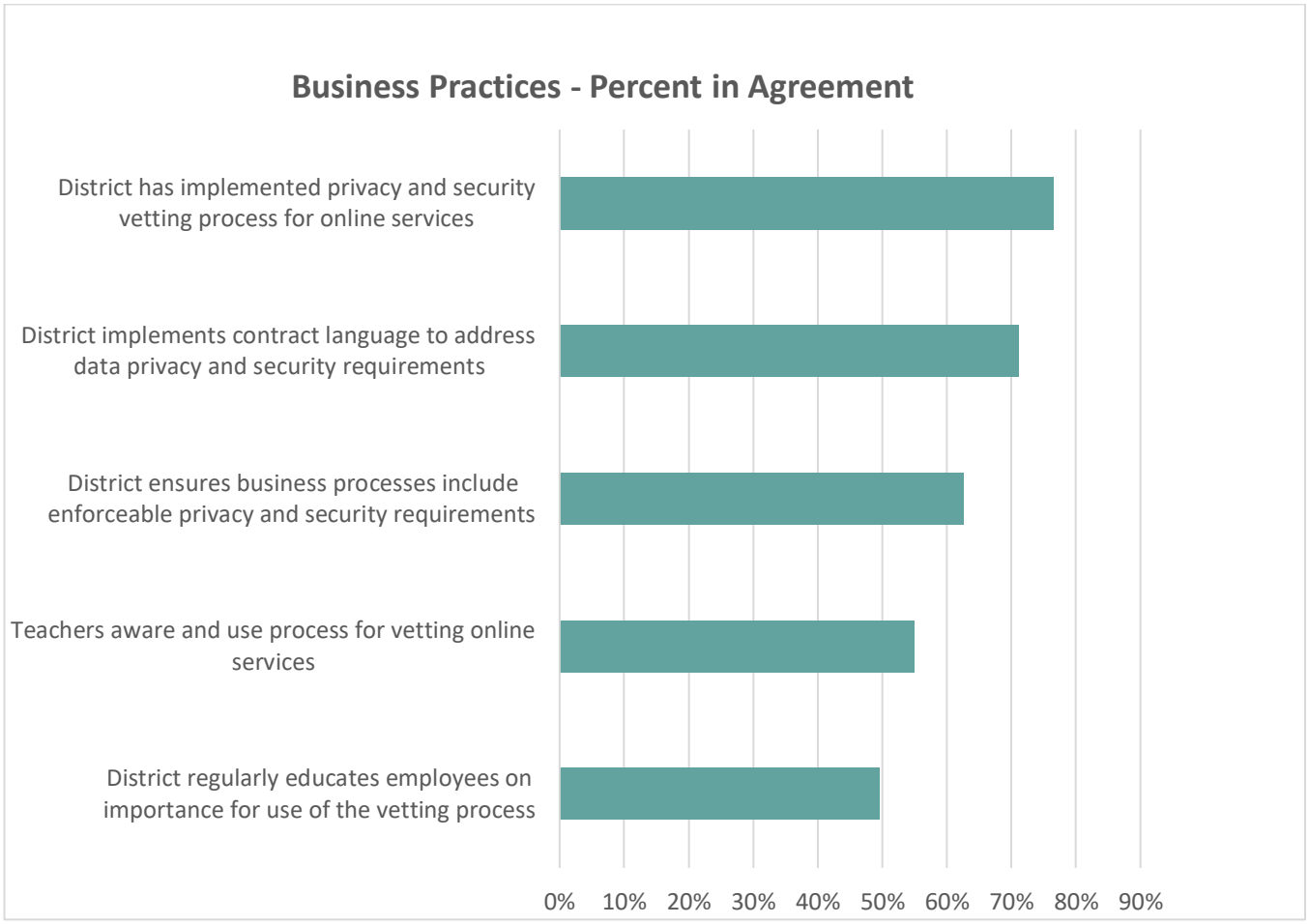
However, bear in mind that when asked direct questions about the existence of specific, foundational privacy policies, training, and other basic requirements that fit within the responsibilities of district leadership - or otherwise within the ability of district leadership to facilitate - a different picture begins to emerge.

Responses to those specific questions echoed findings noted earlier in this report, regarding what concerns district ed tech leaders most about student data privacy, demonstrating that the worries reflect reality.

The contrast between the perception of leadership and stated concerns related to employee management and availability of resources is further illustrated in this report's sections on Data Security/Data Security Policy Management Practices and Professional Development and Classroom Practices.

Business Practices

When considering student data privacy practices related to business functions, participants again gave themselves strong marks: 77% indicated that their district had implemented a process for vetting the privacy and security of technologies before bringing them into the district, and 71% indicated that they ensured data protection agreements were in place with vendors.



However, when looking at these strong numbers, we must also consider that only 55% of respondents indicated that their teachers were aware of and used the vetting process, and only 50% indicated that the district educated its employees about the importance of and expectations for use of the vetting process.

If employees are not aware of and using the vetting process, then technologies are likely coming into the classroom without having undergone a privacy and security vetting assessment, and perhaps also without a data protection agreement in place. Both are foundational necessities.

When we consider, as noted above, that a majority of respondents were concerned about not being able to control the influx of free and low-cost technologies brought into the classroom by teachers, the gap in employee education regarding expectations for and use of the vetting process, as well as the reported limited teacher awareness of and use of the vetting process, comes into sharper focus.

We might consider that districts may be focusing their data privacy and security vetting process on technologies that go through their procurement process. Or, perhaps district ed tech leaders are hindered by the lack of policies and communications articulating to teachers that the vetting process is required, or by a lack of agency to make the vetting process mandatory.

Whatever the driver, when a district does not conduct its own privacy and security assessment of vendor technologies before they are brought into the district, they cannot be fully aware of the potential risks that a particular product may pose to their student data (as well as to employee and parent data), nor can they take all of the necessary steps to properly mitigate those risks.

Data Security/Data Security Policy Management Practices

As noted earlier in this report, the majority of participants indicated that, among other things, their district had up-to-date policies to govern privacy practices and that leadership demonstrated a clear understanding of data privacy and security requirements and ensured adequate resources were in place to support the student data privacy program.

However, when asked questions about whether specific policies and practices were in place, there was a stark difference in responses.

For example, while 67% of participants reported that their leadership had ensured adequate policies were in place to support the student data privacy program, only 48% reported having policies addressing all of the following:

- Data retention for student records.
- Protection (such as encryption) of student data in transit and at rest.
- Controls limiting access to student data (such as rule/role-based access limitations and corresponding technical controls).

While it is possible that some respondents had some of these policies in place and not all of them, the absence of even one of these fundamentals should be cause for concern.

In addition, only 42% reported that their district has enforceable policies regarding storage of data on local computers, mobile devices, storage devices, and cloud file-sharing and storage services. What this means in practice is that employees may be able to move student data into systems where it is not as protected as it is in the primary database. Thus, protecting the student data is less assured; tracking where the data goes becomes more complex, if not impossible for most districts; and the risk of unauthorized access and data loss increases.

On a positive note, 73% of districts gave themselves high marks for having a process in place to communicate privacy and security incidents to impacted individuals and, where applicable, regulators. Since a documented incident response process is fundamental to a data security program (and since such a process should include a protocol for managing communications), this is somewhat encouraging, suggesting that districts have been attending to this critical requirement.

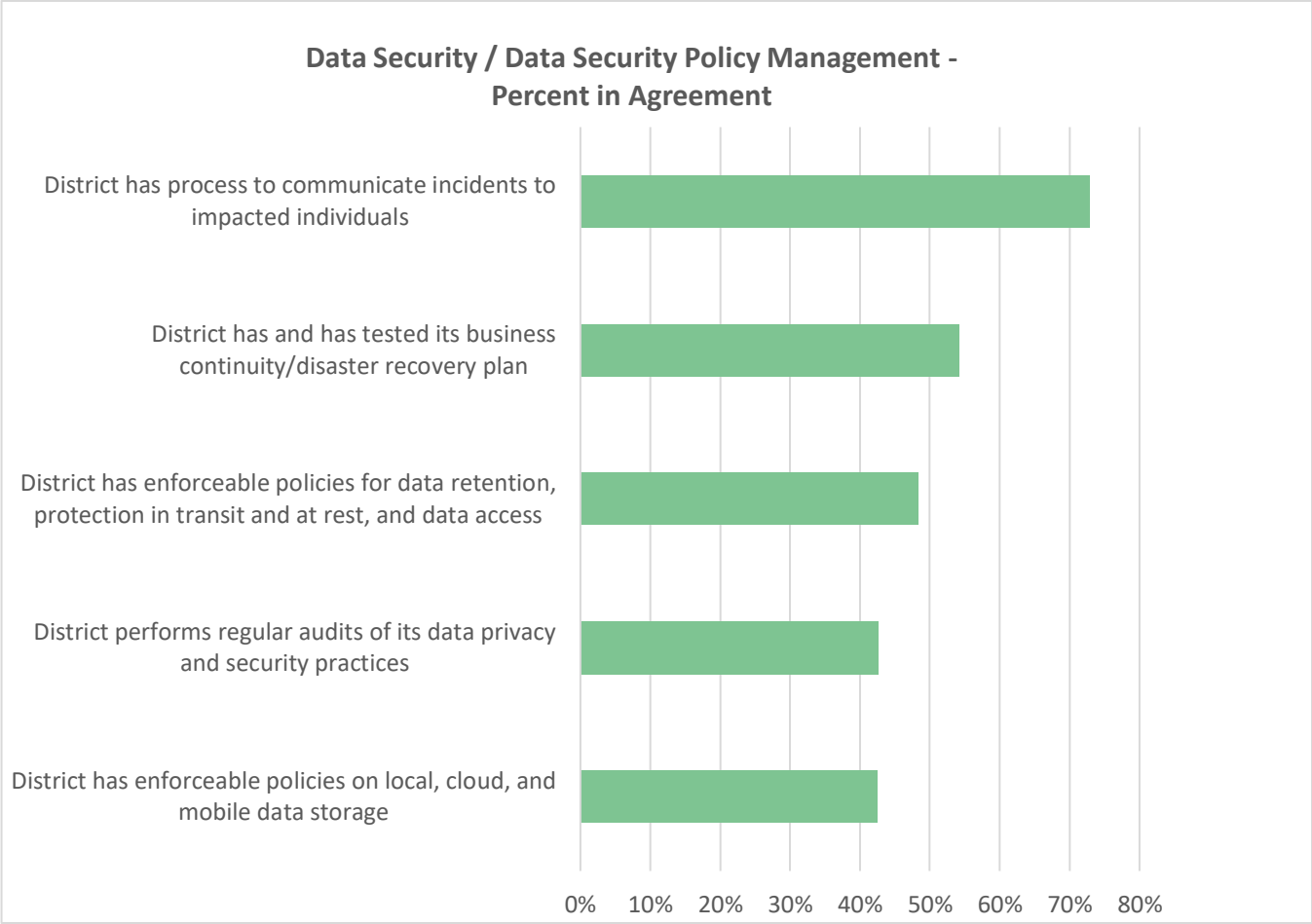
However, only 54% agreed that they had verified and tested a business continuity process. With ransomware running rampant in education,[9] this needs to improve. The overarching data privacy and security programs are the first lines of defense against ransomware. In the event of a successful ransomware incident, a verified, tested business continuity process is the means to help ensure that the incident doesn't disrupt school operations. It is also a necessary component to ensuring continuity of education in the event of natural disasters and other potential system disrupters.

Finally, only 43% of districts reported that they perform an audit of data privacy and security practices on an established, regular basis. While some third-party audits may be financially out of reach for districts, they should at least be considered as part of privacy and security program budgets. At a minimum, if a formal third-party audit truly proves to be unaffordable, districts are encouraged to conduct their own internal reviews in whatever ways are manageable.[10] After all, in the absence of such a review, an institution is hampered in its ability to identify and properly manage gaps, or improve on the existing privacy and security programs in an efficient, meaningful, and effective manner.

---

[9] Homeland Threat Assessment 2024. US 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."

[10] While not a substitute for formal privacy and security program audits, for a simple and free starting point, districts might consider conducting a privacy self-assessment against the CoSN TLE requirements. CoSN's Trusted Learning From the Ground Up: Fundamental Policies and Procedures Every District Should Have in Place can also serve as a point of comparison for policy libraries. Security assessments should be conducted by leveraging nationally recognized cybersecurity frameworks, such as the NIST Cybersecurity Framework.



In short, developing, implementing, and enforcing a foundational set of privacy and security policies would seem to deserve much more attention than is currently being paid.

To put a finer point on the potential leadership gap here, in many districts, policy development is the purview of the superintendent and board, while processes designed to implement the privacy and security policies are the purview of ed tech leaders.

However, that doesn't mean that superintendents and boards need to become experts in student data privacy and security. In fact, a number of districts have reported that while policy development is the responsibility of the superintendent and the board, ed tech leadership is empowered to draft "guidance" and "data governance manuals" that have the weight of policy. This model relieves the superintendent and board of some of

the knowledge burden that is necessary to properly draft policies in these specialty areas. It also allows the drafting to be more effectively managed by those who will be responsible for implementing the policies.

However, any such documentation must have the formal weight of policies. This means that the superintendent must work in partnership with ed tech leadership to help clear hurdles that will then allow ed tech leadership to 1) develop the needed privacy and security guidance and governance manuals, and 2) establish the implementation and enforcement authority.

Professional Development and Classroom Practices

The survey responses to questions related to professional development and classroom practices also revealed some opportunities for improvement.

For example, likely guided by requirements of the Children's Internet Protection Act (CIPA), 66% of districts reported that their teachers implement a curriculum to promote student information literacy, digital citizenship, and internet safety.[11] Often, we now see that curriculum including data privacy lessons.

However, with respect to privacy lessons for staff, only 45% reported that all staff members participate in annual student data privacy training related to applicable federal and/or state laws. When looking at training and professional development

[11] Federal Communications Commission (FCC). Children's Internet Protection Act (CIPA). Schools subject to CIPA must, as required by the Protecting Children in the 21st Century Act, "provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response."

designed specifically for different areas of school operations and academics, only 38% reported that privacy and security of student data was included in that training.

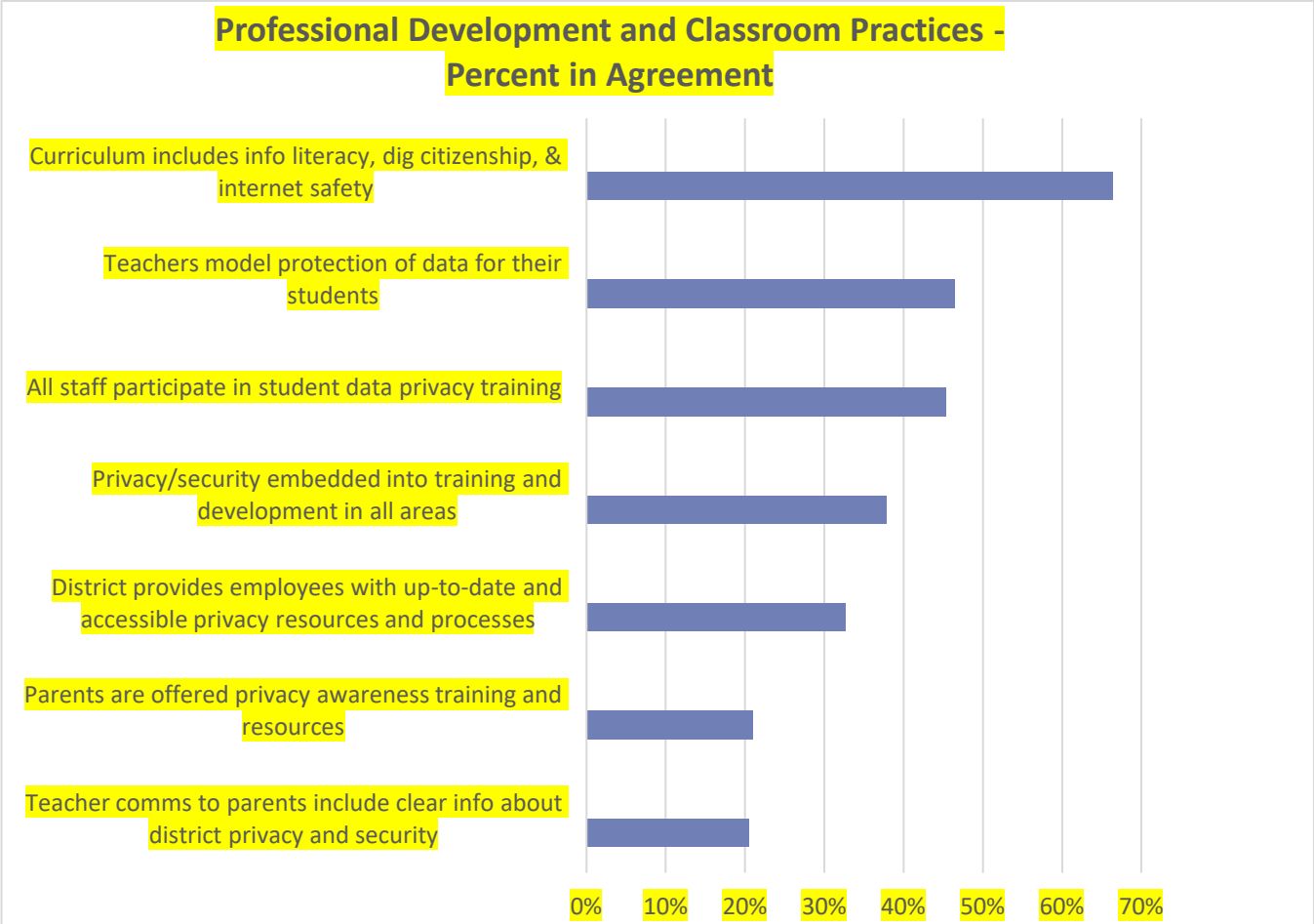
Just 33% reported that their district provided employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.

All employees need to be trained on the importance of protecting student data, requirements of applicable laws, and how to implement district privacy and security policy requirements in their work.

However, there is an inherent challenge for ed tech leaders to be able to deliver employee privacy training in an environment in which they are not empowered to require it and have limited opportunities to engage with other departments that may help to facilitate securing the time needed for employees to participate in the training.

With respect to providing training for teachers, the situation is further complicated by the fact that educators are already required to engage in extensive professional development requirements for licensing and relicensing. Adding to those existing requirements is a challenge. However, given that teachers handle student data every day, student data privacy training should be mandatory.

Again, there are opportunities for superintendents to help break down organizational silos and otherwise remove obstacles to implementing such training.



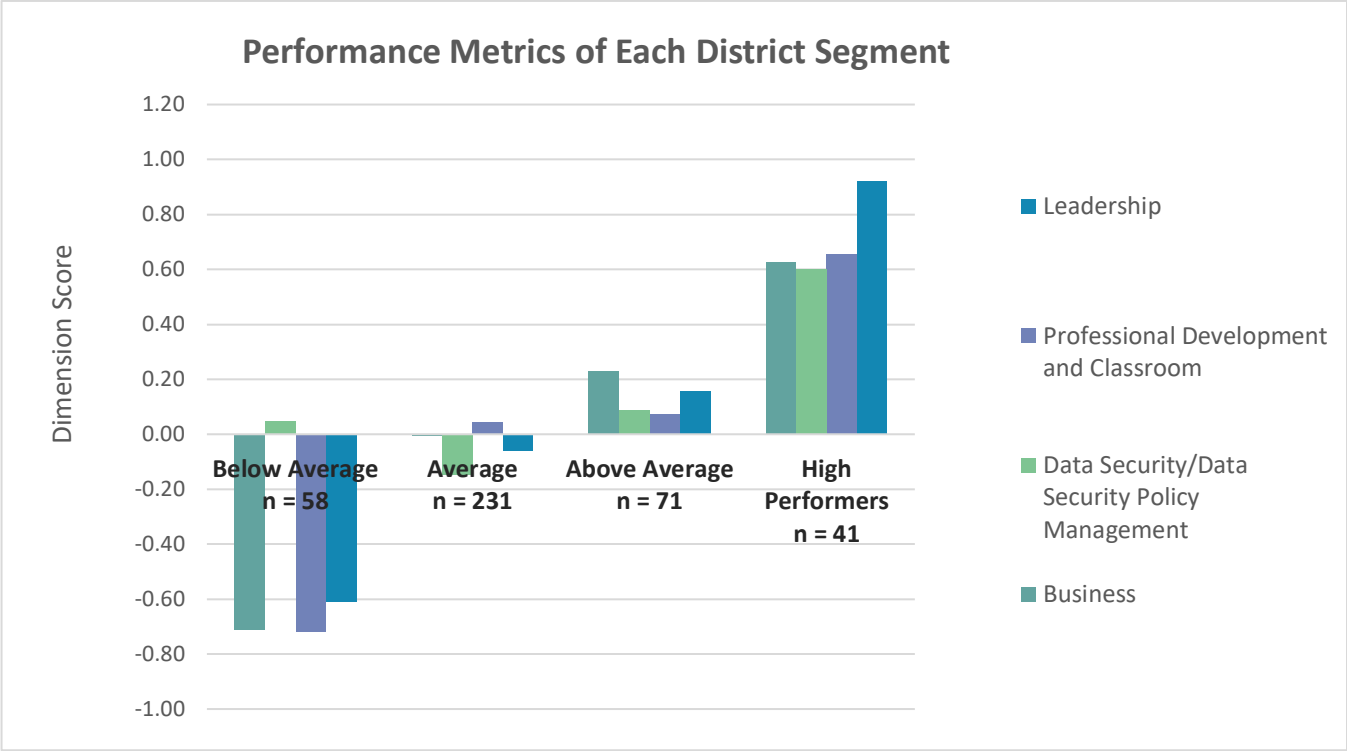
Student Data Privacy Performance and District Characteristics

As noted in the Methodology section,[12] to further analyze the findings, different psychographic segments were created among participants, based on their privacy performance. Those privacy performance segments are as follows:

[12] See Appendix B and Appendix C for more information on the analysis and segmentation.

- **High Performers:** This segment of districts is defined by their high performance scores on Leadership, Security/Security Policy Management, and Professional Development and Classroom Practices. That is to say, when asked questions about those practices, those districts generally gave themselves high scores, reflecting strong student data privacy practices.[13]
- **Above Average:** This segment of districts is defined as having the strongest performance scores with respect to Business Practices, and are just above average performance in all other areas.
- **Average:** This segment of districts performs moderately in all areas, suffering the most in Security/Security Policy Management practices.
- **Below Average:** This segment of districts suffers in all areas except Security/Security Policy Management practices.

[13] Districts that have earned their CoSN TLE Seals or that have indicated that they are working toward obtaining one were far more likely to be High Performers than other districts. Those who are not working on getting a CoSN TLE seal or don't already have one were significantly more likely to be Below Average in student data privacy performance. For more information on performance of districts that have earned the CoSN TLE Seal as compared with other survey participants, please see Part 2 - 2025 National Student Data Privacy Report: CoSN Trusted Learning Environment Perspectives.



Note: In this chart, positive numbers reflect above average performance relative to other survey participants across the different dimensions and negative numbers reflect below average performance. There is no visible score for Average performers in Business Practice because the score is at 0 (average).

We then considered district performance segments in relation to district requests for guidance, barriers to improvement and opportunities for improvement. This allowed us to examine whether and what differences existed in student data privacy program barriers and needs for districts currently operating at different performance levels.

Requests for Guidance

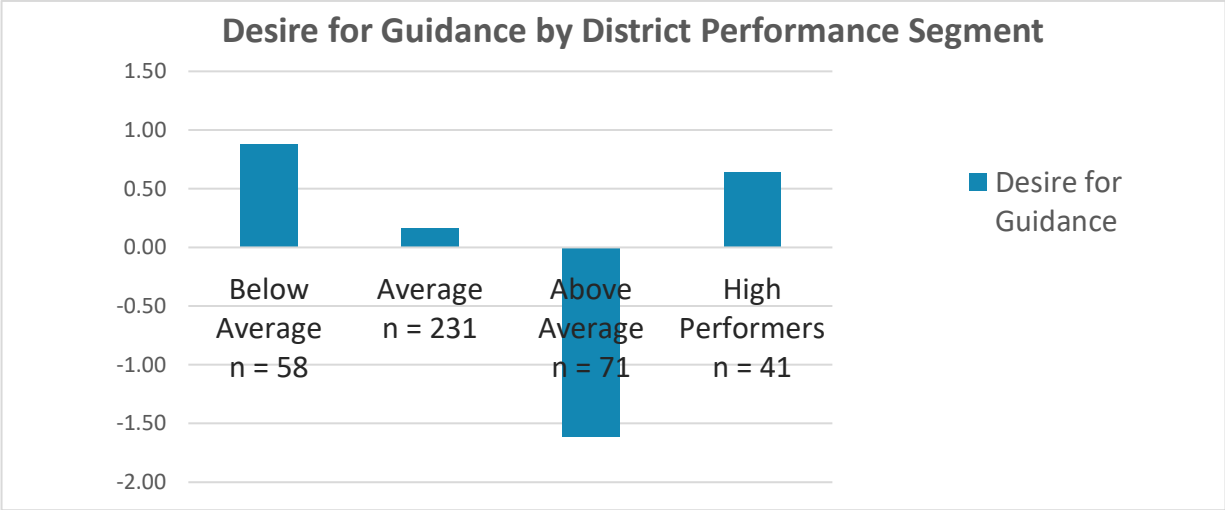
As previously noted, respondents were near-universal in requesting more guidance on building and improving their district student data privacy program. All options provided in the survey - guidance on implementing federal and state privacy laws, policy templates provided by states, guidance on implementing specific privacy practice requirements, training, and help prioritizing the work with the superintendent - deemed helpful by between 62%-82% of participants.

Clearly a good deal of additional guidance is needed to support development and implementation of strong student data privacy programs. In some cases, this means more information on federal and state law requirements. However, it also means providing guidance on how to implement processes that address those requirements. Understanding what a law requires and translating that into procedure that meets those requirements are two different skill sets. Both are needed.[14]

When looking at the desire for guidance within each performance segment, the High Performers continued to have a strong desire for guidance, perhaps reflecting an understanding that data privacy work is a risk mitigation discipline, requiring constant improvements in maturity of practices, as well as an ability to apply fundamental privacy concepts to new and emerging technologies.

They were bested in a desire for more guidance only by the Below Average performers. (Interestingly, Above Average performers were less likely to indicate a desire for more guidance. It's possible that some of these districts have reached a certain level of maturity but have not yet tapped into the broader community of privacy and security experts that would open the door to the next level of work.)

[14] CoSN's Student Data Privacy Initiative now provides resources on implementing certain student data privacy practice requirements.



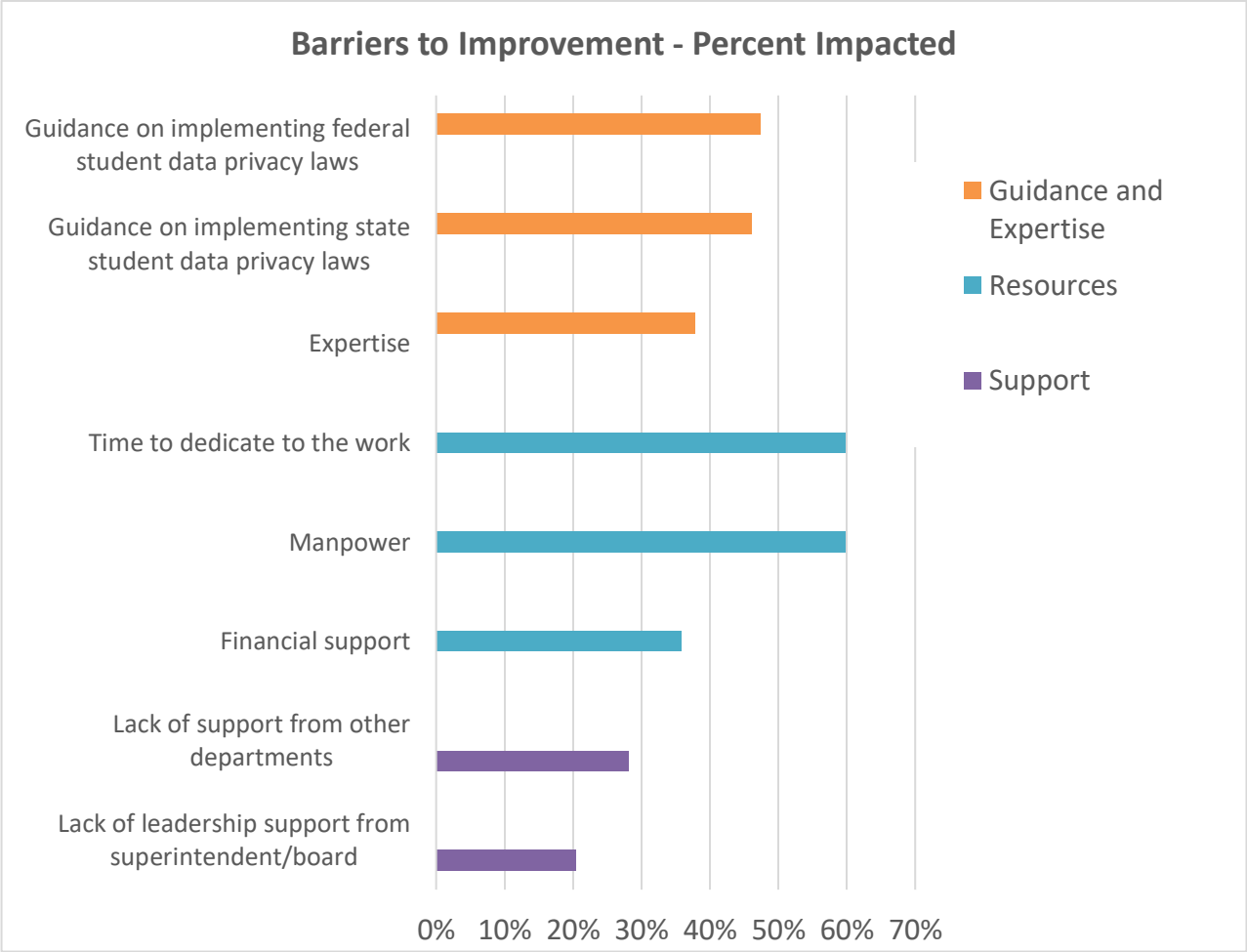
Note: In this chart, positive numbers reflect a stronger degree of desire for guidance among survey respondents, while negative numbers a lesser degree of a desire for guidance.

Barriers to Improvement

Across all respondents, regardless of where their districts fell with respect to level of performance around the student data privacy program, the most frequently indicated barriers to improving student data privacy programs were time and manpower, each cited by 60% of respondents. Considering that ed tech leaders are commonly doing the job of a technology leader, a privacy leader, and a security leader, this should come as no surprise. (In the chart on page 34, time, manpower, and financial needs are collectively referred to as Resources.)

A need for guidance on federal laws (47%), state laws (46%), and privacy expertise generally (38%) - collectively referred to as Guidance and Expertise in the chart - were more frequently cited as barriers than financial resources, which was cited by 36%.

Survey results show 20% of respondents cited lack of support from their superintendent as a barrier to the work, while 28% cited a lack of support from other departments, something that could be eased via support from the superintendent. This is collectively referred to in the following chart as Support.

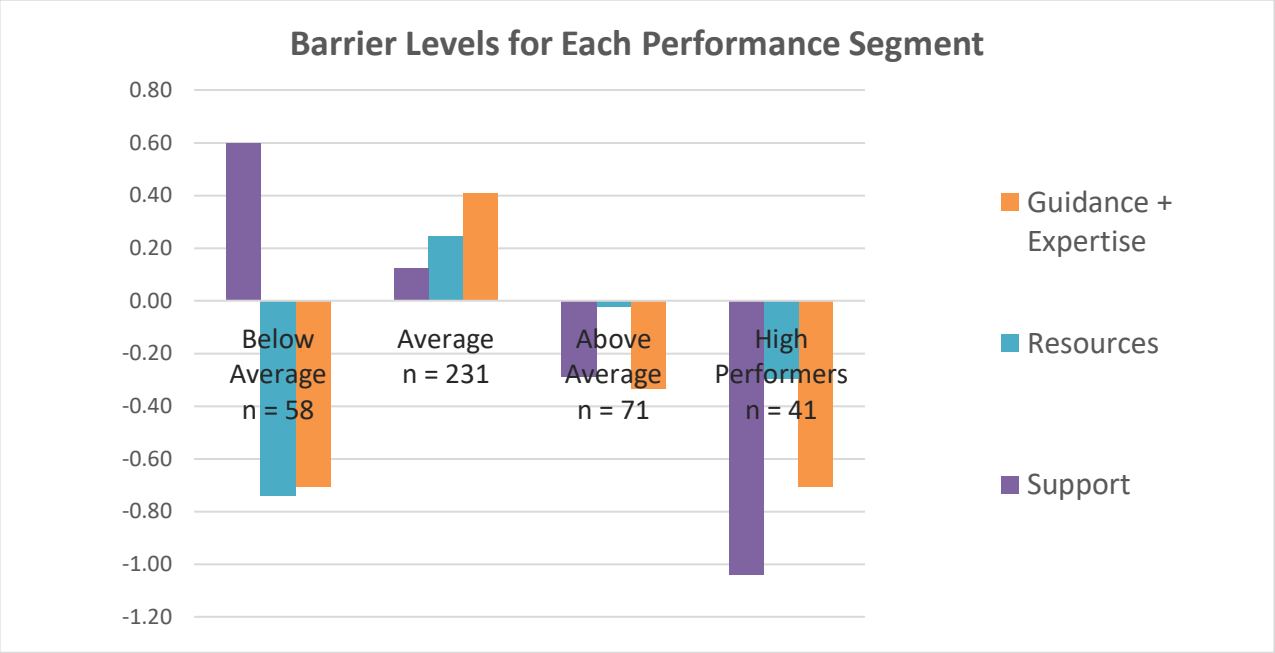


It's important to note that ed tech leaders are generally conveying that their work as privacy leaders is not only under-resourced from a manpower perspective, but also that training and leadership support could go a long way in driving improvements in district student data privacy programs.

When considering the barriers noted above in relationship to the different performance segments, barriers were found to be a key differentiator across the groups.

- **Above Average** and **High Performers** differ in their access to Resources, and not surprisingly, High Performers reported having fewer or less impactful barriers in relation to their needs for Support and Guidance.
- **Average** districts reported having barriers in all three areas.

- **Below Average** districts dominated in reporting a lack of sufficient Support from other departments and from leadership.



Note: In this chart, positive numbers reflect the relative strength of the impact of a barrier, while negative numbers represent the relative weakness of the impact of a barrier or the absence of a barrier.

Opportunities for Improvement

The lowest scores for district leadership came in relationship to questions about transparency with the community. Thus, for some, the simple acts of making district policies readily available to community members on the district website, and providing community members with transparent, updated, and accessible communications regarding the collection, management and use of student data would improve their overall student data privacy profile.

However, as noted above, there are more challenging areas where leadership needs to focus to support the substance of the student data privacy program. Ensuring that the work is properly prioritized and resourced, emphasizing the importance of the work to all employees, breaking down departmental silos to ensure that privacy work is supported by all departments, and partnering with ed tech leadership in developing a

comprehensive set of privacy and security policies as the framework for the privacy and security programs[15] would likely result in the most substantive impact on student data privacy. The policies - along with clear communications about ways in which the district uses, shares, and protects student data might then be made available to the community.[16]

Privacy Performance and Regional Socioeconomic and Demographic Measures

The level of student data privacy program performance was also considered in relation to various regional socioeconomic and demographic measures as provided by the U.S. Census, including area economic indicators, district size, urbanicity, geography, and ethnic makeup. The relationship between these measures and district privacy performance were examined as described below.

Economic Indicators

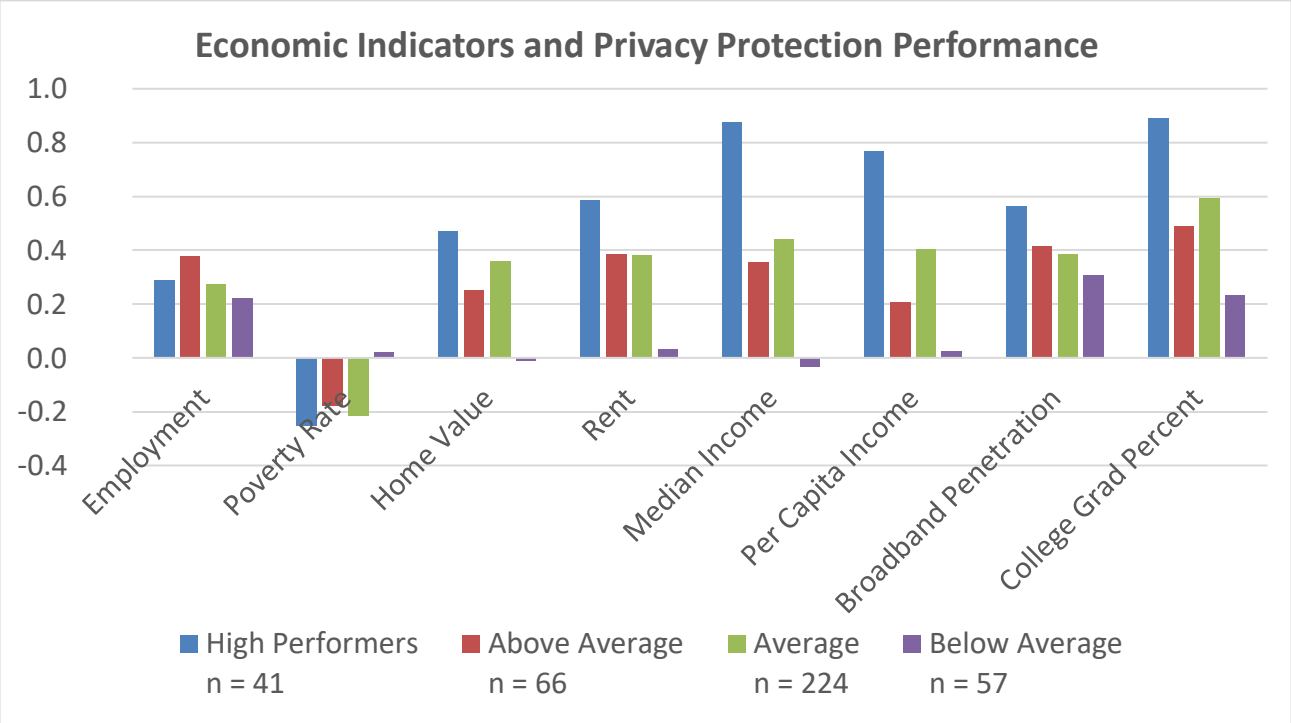
An examination of specific economic indicators revealed a general trend in which we see that higher performing districts tend be in areas with high economic status levels. As illustrated in the chart on the next page, with the exception of broadband penetration, all of the selected economic indicators show a statistically reliable effect. For example, districts that fall into the category of High Performers in relation to their student data privacy programs were consistently shown to be in areas where home values, rent,

[15] For security, see NIST Cybersecurity Framework as an example.
[16] This is not intended to suggest that information that - if made public - would put district systems and student data at risk should be publicly available, but rather that districts should provide clear, accessible, transparent communications about the data privacy program to the community at the level that is appropriate for public consumption in that doing so does not create risk.

median income, per capita income and percentage of college graduates is high, while poverty rates are low.

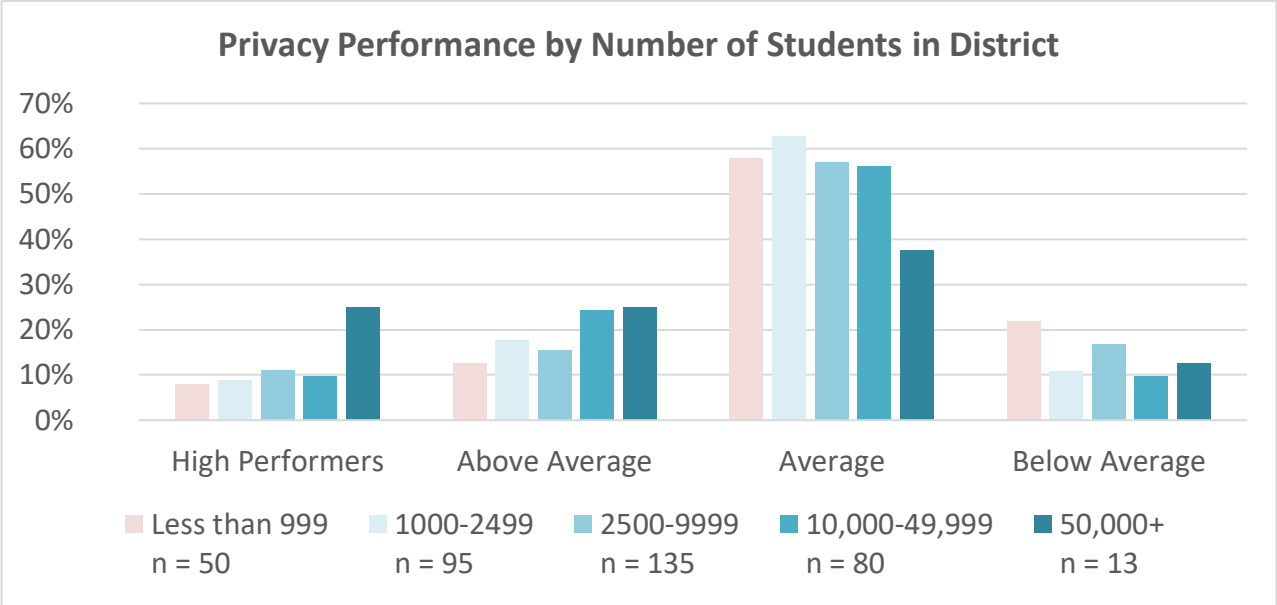
Overall, districts that are in the category of Below Average performers with respect to their privacy performance tend to be in areas with lower economic indicators.

In summary, there is an overall trend indicating that the stronger the economic region, the more likely the district is to perform better with respect to student data privacy.



District Size

Overall, there's a general trend in which larger districts with more students are more likely to have better student data privacy program performance than smaller districts. Districts with 50,000 or more students are more likely to be High Performers than smaller districts at a level that is statistically significant.



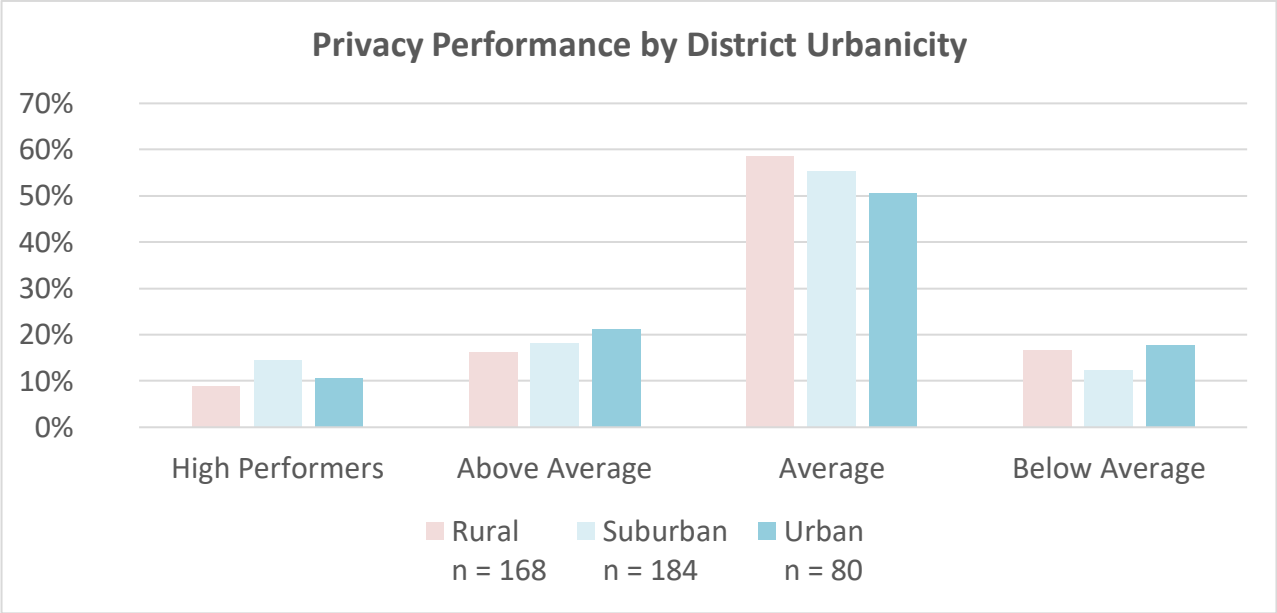
Note: In this chart, the bar demonstrating the percentage of High Performers with 50,000+ students is statistically significant at the 95% confidence level.

Urbanicity

High performing districts tend to be in suburban areas at a level that is statistically significant compared with their appearance in urban and rural areas. There is also a general trend suggesting that Above Average districts tend to be in less rural areas.

Average districts trend towards more rural regions, however the data behind those trends are not statistically significant.

Below Average districts show the opposite pattern to High Performers, where suburban areas are less likely to include districts that are Below Average in student data privacy performance.



For more information about regional demographics and the relationship to district privacy performance, see Appendix B.

Conclusion

Despite all the attention that has been paid to student data privacy over the past decade and beyond, we've not previously had the benefit of a data-driven analysis of what districts are doing to build and improve their student data privacy programs, where the challenges lie, and what those responsible for the work really need in order to be successful.

It is our hope that this report, which details the survey findings, helps all interested parties - including districts, state education agencies, parents, and our peer groups that also provide supports for districts - better understand some of the challenges faced by school districts in building and improving their student data privacy programs, and how we might begin to approach addressing those challenges.

As the survey results illustrate, the road ahead to helping districts improve their student data privacy programs is complex. Currently, data privacy as a function is not typically

elevated within school districts in a manner that reflects its importance. Indeed, often references to a responsibility to build a program designed to support compliance with federal and state laws isn't even mentioned in the applicable job description. Student data privacy training is generally lacking for those responsible for designing the student data privacy program and for employees who handle student data every day. In addition, ed tech leaders are sometimes still in a position in which they need to convince a superintendent that the work matters.

This must change.

Perhaps the first challenge to address is the apparent disconnect between perception of leadership performance around the work and the reality of the student data privacy practices that are in place. In some cases, the data may give us clues about why those gaps exist.

For example, without privacy responsibilities codified into an edtech leader's job description, it's possible that superintendents and ed tech leaders themselves have different perceptions of who is responsible for what privacy work.

Some superintendents may believe they are providing everything necessary to create an effective student data privacy program. They may not be aware if their ed tech leaders are struggling to manage employee behavior or are not getting the support they need from other departments.

In other cases, it may be a lack of awareness that building an effective student data privacy program requires engagement by all employees across multiple departments. Once that is understood, it becomes clear that in education institutions - as is the case in all organizations - addressing the needs starts with organizational change management to enable the work to progress and for all the necessary pieces of a student data privacy program to be put in place.

Setting the stage to establish the importance of student data privacy work within a district does not require the purchase of an expensive tool or technology. Instead, the first requirement is that, collectively, attention be paid in a way that emphasizes the importance of the work across the institution, and that supports ed tech leadership in effectuating the necessary organizational change.

In short, district leadership must[17]:

- Recognize the work of building and improving a student data privacy program as leadership imperative.
- Emphasize the importance of the work with all employees, and create updated job descriptions that reflect the importance of the work for those responsible for building and implementing student data privacy programs.
- Ensure that the student data privacy program is adequately resourced - including with adequate policies - and provide training necessary for ed tech leadership to succeed in the work.
- Support ed tech leadership in breaking down institutional silos to more effectively implement student data privacy requirements across teams, including by mandating privacy and security training for all employees.
- Ensure that all district employees adhere to district policies with consistent enforcement of those policies.

In turn, district ed tech leaders must ensure that they are communicating upwards within the institution in a way that clearly articulates what they need from their superintendents to better support the work.

---

[17] For more information, see the CoSN EmpowerED Superintendent Initiative resources, "Student Data Privacy. A School System Priority. An Essential Commitment" and "The Role of Leadership in Protecting Student Data Privacy."

By attending to this work in a way that addresses the organizational components that form the backbone for any successful privacy program, we can bring meaningful, substantive improvements to district student data privacy programs, strengthening protections for students nationwide.

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

About the Survey Respondents

Survey respondents came from 39 states and the District of Columbia.[18] 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.).[19]

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

[18] 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.

[19] 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.

- 7%: 51-100 schools
- 12%: 21-50 schools
- 39%: 6-20 schools
- 40%: less than 5 schools

Free and reduced-price lunch percentage[20]:

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

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

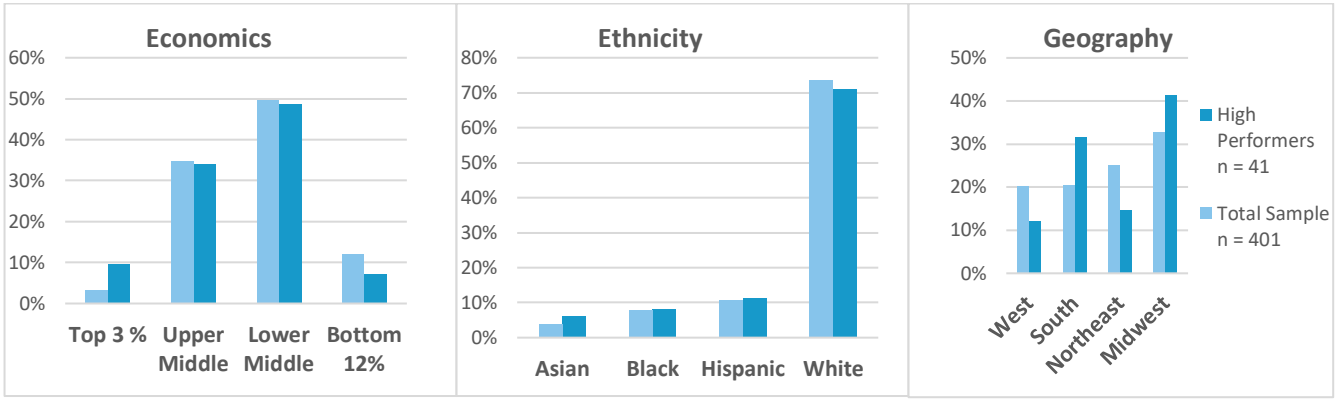
[20] While free and reduced lunch percentage is often used as a stand-in for poverty rates, we have not used it as such in this report and provide it only in furtherance of participating district profiles.

Appendix B

More on Demographics and Privacy Performance

Demographic Characteristics of High Performing Districts

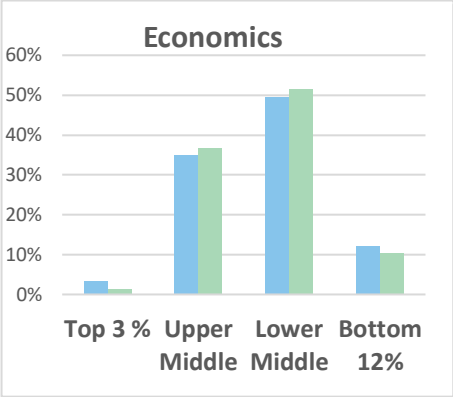
- Economics: There was a tendency for High Performers to appear more often in regions that are in the top 3% economically, relative to other survey participants, and less often in the bottom 12%.
- Ethnic composition: This was not correlated with the High Performer category - composition of the High Performer districts matched the overall sample very closely.
- Geography: There was a tendency for High Performers to appear more often in the Midwest and South, and less often in the West and Northeast, but these differences were not statistically reliable.

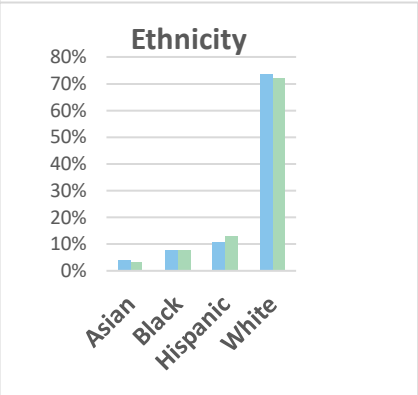


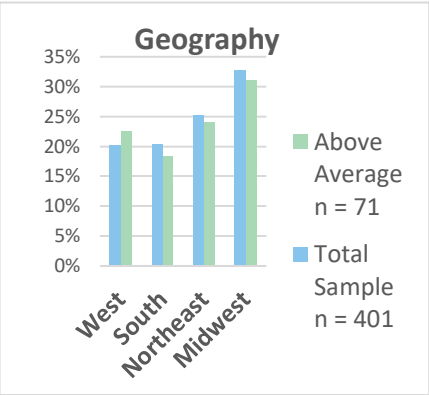
Note: In the Economics chart, data on the Top 3% is statistically significant at the 95% confidence level.

Demographic Characteristics of Above Average Performers

- Economics: There was a slight tendency for Above Average districts to appear more often in the Upper Middle areas, and less often in the Bottom 12%, but these differences were not significant and there is no general trend suggesting that Above Average districts appear in areas with superior economic levels.
- Ethnic composition: This was not correlated with the Above Average districts - ethnic composition closely matched the overall sample very closely.
- Geography: Above Average districts matched the geographic distribution of the overall sample.



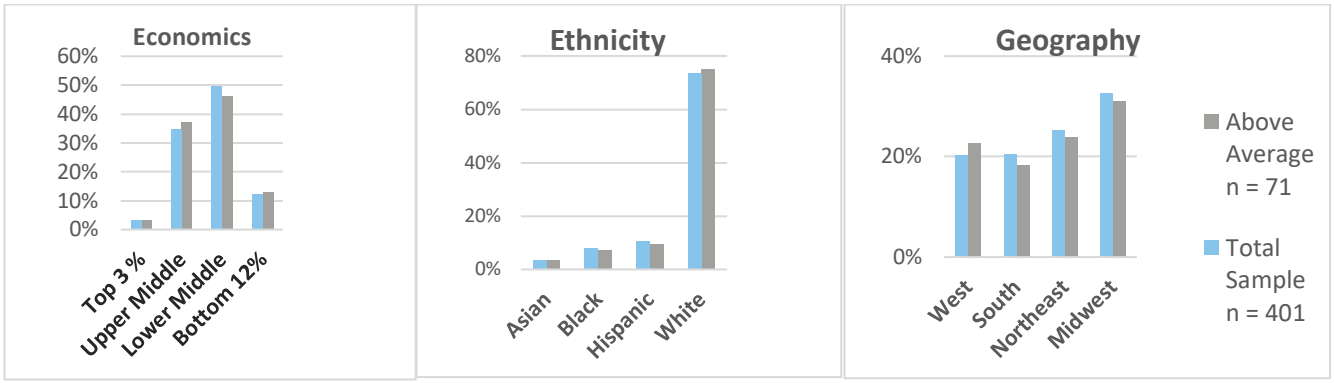




Demographic Characteristics of Average Performing Districts

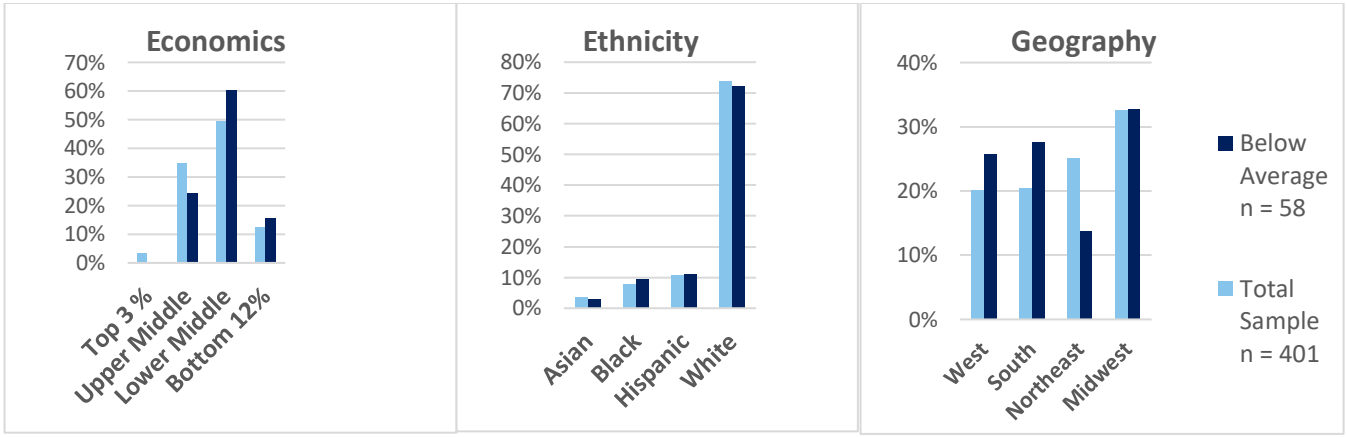
- Economics: There was a slight tendency for Average districts to appear more often in the Upper Middle areas, but these differences were not significant and there's no general trend indicating that Average districts appear in areas with superior economic levels.
- Ethnic composition: Average districts were somewhat less ethnically diverse than the overall sample, but these differences were not statistically reliable.

- Geography: Average districts matched the geographic distribution of the overall sample.



Demographic Characteristics of Below Average Districts

- Economics: There was a trend for Below Average districts to be situated in areas with lower economic indicators, but these differences were not statistically significant.
- Ethnic composition: This was similar to the overall sample for Below Average districts.
- Geography: Below Average districts matched the geographic distribution of the overall sample.



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 student data privacy programs, and not about district 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.

Statistical segmentation was applied as part of the analysis, dividing districts into distinct groups based on common characteristics, each containing different dimensions.[21] 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 respondents into four distinct groups: (1) High Performers, (2) Above Average, (3) Average, and (4) Below Average.

2. **Economic Segments:** Economic segmentation for regions 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. Segments of 1) Top 3%, 2) Upper Middle, 3) Lower Middle, and 4) Bottom 12% among survey respondents were created based on the relative economic performance of the regions.

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:

Variable Code	Description	Variable Code	Description
B01003_001	Total Population	B24011_006	Population in Computer, Engineering, and Science

[21] 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.

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.[22]

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 Practices.

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

[22] 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.

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.

In addition, for Part 2 - 2025 CoSN National Student Data Privacy Report: Trusted Learning Environment Perspectives, we compared responses from districts that were CoSN Trusted Learning Environment (TLE) Seal recipients with districts that were not to consider and to illustrate differences in the results.

We also interviewed ed tech leaders from districts that are CoSN TLE Seal recipients to learn 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 available in Part 2 - 2025 CoSN National Privacy Survey: CoSN Trusted Learning Environment Perspectives.

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

Appendix D

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.

For more on the CoSN TLE Seal requirements, see the CoSN TLE Examples of Evidence.

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, as well as for their support in finalizing this report.

About the Author

Linnette Attai is project director for CoSN's Student Data 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.