



Out of Sight, Out of Mind?

**School Districts' EdTech Efforts Have
Outpaced Transparency and Student
Privacy**

Elizabeth Laird
Maya Lagana, Independent Contractor

November 2022



The **Center for Democracy & Technology** (CDT) is a 27-year-old 501(c)3 nonpartisan nonprofit organization that fights to put democracy and human rights at the center of the digital revolution. It works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

Out of Sight, Out of Mind?

School Districts' EdTech Efforts Have Outpaced Transparency and Student Privacy

Authors

Elizabeth Laird

WITH CONTRIBUTIONS BY

Maya Lagana, Independent Contractor

SUGGESTED CITATION

Elizabeth Laird & Maya Lagana, *Out of Sight, Out of Mind?: School Districts' EdTech Efforts Have Outpaced Transparency and Student Privacy*, Center for Democracy & Technology (Nov. 2022) <https://cdt.org/insights/report-out-of-sight-out-of-mind-school-districts-edtech-efforts-have-outpaced-transparency-and-student-privacy/>.




This report is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Contents

| | |
|---|-----------|
| Introduction | 5 |
| Key Findings | 7 |
| Finding #1: LEAs are transparent about staffing but appear to lack capacity dedicated to student privacy. | 7 |
| Finding #2: LEAs post information regarding their legal obligations but do not provide additional information about their efforts to protect students' privacy. | 8 |
| Finding #3: LEAs provide technology resources aimed at the devices they provide but privacy-specific resources are very rare. | 10 |
| Recommendations for Education Leaders | 12 |
| State Education Agency Actions | 12 |
| Local Education Agency Actions | 12 |
| Conclusion | 14 |
| Appendix: Methodology | 15 |
| State Selection | 15 |
| Sampling Methodology | 15 |
| Data Gathering | 15 |
| Data Verification | 15 |
| Endnotes | 16 |

Introduction

As the use of technology in education and corresponding privacy concerns have increased, dedicating appropriate staff to protect student privacy has become essential.



The use of data and technology in education has increased substantially in recent years, and, along with it, has come increased attention on the need for education agencies to protect student privacy. This is not a new responsibility. For decades, education leaders have been legally responsible for protecting student information, beginning with the enactment of the main federal student privacy law that protects student data, the Family Educational Rights and Privacy Act (FERPA) of 1974.

But these legal requirements are no longer sufficient to fully protect student privacy. As this report discusses in detail, research conducted by the Center for Democracy and Technology (CDT) has found that education agencies do not have fully dedicated staff and resources to meet these increased obligations.

As the use of technology in education and corresponding privacy concerns have increased, dedicating appropriate staff to protecting student privacy has become more essential. Research suggests that 95% of security incidents are at least partially the result of human error, underscoring the importance of allocating and building staff capacity.¹ Historically, privacy responsibilities have been distributed over multiple departments without clear ownership. This results in unclear roles, lack of accountability, and the absence of an organizational strategy on how to balance the benefits of data and technology with privacy risks.²

In addition to staffing, it is vital that families and other stakeholders understand their rights and potential risks related to student privacy. While federal and, in many cases state, laws give students' families significant rights³ to protect their children's privacy in schools, research shows that families do not fully understand these rights.⁴ In addition to raising awareness of legal rights, additional transparency and public-facing resources can support meaningful engagement with communities, establish public trust, and proactively address parents' questions and concerns. Without these elements, governments can trigger a backlash that prevents data from being used effectively by education organizations.⁵

To assess local education agencies' (LEAs)⁶ progress, CDT examined publicly available information about student privacy staffing and transparency decisions in 43 LEAs of various sizes, geographies, and socioeconomic status in four states. CDT wanted to understand what information is transparently and proactively available to families, staff, and other stakeholders.

The scope of this research is primarily focused on LEA practices but also examines the relationship between LEAs and their state education agency (SEA). CDT research shows that families are much more likely to look to their LEA for resources, but SEAs can provide support to LEAs in doing this work.⁷ Therefore, it is important to understand LEA practices, as well as how states are supporting them.⁸



Key Findings

LEAs' staffing and transparency efforts have not kept pace with their large investments in education technology and expanded data collection. In particular, this research revealed that LEAs generally:

- Are transparent about staffing but lack capacity dedicated to issues of privacy;
- Post information regarding their legal obligations but do not provide additional information about their efforts to protect students' privacy; and
- Provide cursory education technology resources, but privacy-specific resources are very rare.

Finding #1: LEAs are transparent about staffing but appear to lack capacity dedicated to student privacy.

As previously stated, the vast majority of security incidents are at least partially the result of human error. A remedy to help prevent human error is to allocate staff specifically to student privacy and security as an LEA builds organizational capacity to effectively implement policies and practices that keep pace with edtech growth. Additionally, allocating staff and resources to issues of privacy sends a signal to all staff as well as the public about the importance an organization places on protecting students. Finally, state and federal laws give families certain rights over their students' data, and having dedicated staffing can help ensure families are afforded those core rights.⁹

Analysis of LEAs' and SEAs' websites and other publicly available information reveals areas of progress, as well as gaps in staffing and transparency:

Progress:

- LEAs are very transparent about staffing, with most publicly sharing staff directories that include information about all of their employees. They are posted online and typically include names, titles, departments and contact information. The staff directories are also consistent across LEAs within the state, indicating coordination across LEAs and/or with the SEA.
- Most LEAs, regardless of size, have at least one full time staff member dedicated exclusively to the use of technology (e.g., Director of Technology, IT Network Analyst).

Allocating staff and resources to issues of privacy sends a signal to all staff as well as the public about the importance an organization places on protecting students.



Key Findings

Gaps:

- Regardless of size, LEAs do not have staff obviously dedicated to privacy, security, or data governance as evidenced by having titles denoting these issues.¹⁰ Moreover, most LEAs have very small (1-2 people) technology teams, and many do not have any staff focused on data (e.g., database administrators, data analysts).
- None of the LEAs clearly posts a contact for public stakeholders and families to whom they can direct privacy questions or concerns. Contact information for a general IT help desk for LEA staff (and occasionally students) was often the only contact information related to technology.

Leading Example

Oneida School District in New York clearly denotes the District Privacy Officer on their [website](#) as a point of contact, as well as the State's Chief Privacy Officer.¹¹ This information, along with other key information, is listed in a subsection of the "Parent Resources" web page entitled "Data Privacy." It includes district and state policy, approved vendors and links to other resources. This arrangement is common amongst districts in New York, another example of the importance of state guidance.

Finding #2: LEAs post information regarding their legal obligations but do not provide additional information about their efforts to protect students' privacy.

Although data privacy laws, such as FERPA, have granted families rights for decades, this information is not often readily available or understood by parents. This, in turn, means families often do not understand how to exercise these rights.¹² Additionally, the uses of data and technology in education have evolved substantially since these laws were passed. Practically speaking, this has resulted in LEAs needing to implement policies and procedures that go beyond legal obligations in order to fully protect students' privacy.

Analysis of LEAs' and SEA's websites and other publicly available information reveals areas of progress, as well as gaps in staffing and transparency:

There are differing levels of information and details regarding guidance for parents on how to access student records, opt-out of directory information, or in general exercise their rights under FERPA.

Progress:

- All LEAs have some mention of their legal obligations under FERPA on their websites, including the annual opt out process for sharing directory information without parental consent.¹³ This finding aligns with the recent U.S. Department of Education's (ED) study focused on these obligations.¹⁴
- Within states, the language used to discuss FERPA and other privacy obligations is highly consistent across LEAs. FERPA-specific language is frequently taken from the ED model language,¹⁵ underscoring the importance of federal support.
- Additionally privacy requirements specific to a state also are described using highly consistent language and are provided in similar formats (e.g., LEA board policy or handbook). This suggests a willingness of LEAs to follow guidance issued by the SEAs and further emphasizes the potential role for SEAs to provide student privacy support. Finally, this consistent language and resources is also true for some policies that go beyond legal obligations (e.g., privacy of mental health data) that are present and consistently-messaged in all LEAs within an individual state.

Gaps:

- FERPA and other privacy-related policies are difficult to find on LEA websites. Oftentimes, this information is just a few paragraphs within lengthy student handbooks and/or board policies rather than standalone website content that is easy to find. This is true across LEAs regardless of size. Board policies in particular are challenging, as they are not a document parents would often reference.
- There are differing levels of information and details regarding guidance for parents on how to access student records, opt-out of directory information, or in general exercise their rights under FERPA. Many LEAs only had a statement about these rights without details on how these rights could be exercised, although some SEAs did provide more information.
- Additionally, there is little description of policies and procedures that go beyond legal obligations in protecting students' privacy. Examples of policies that would be helpful to parents and the public to better understand LEA efforts include but are not limited to disclosures around student activity monitoring software (and other tools that surveil students), information about third parties with whom student information is shared, and data deletion policies that prevent the creation of permanent student records, all of which are critical elements of responsible data use.¹⁶

Key Findings

- Very few LEAs publicly post technology plans, with or without privacy specific information, although more do reference these details in board minutes or other materials. This suggests that proactive technology planning may exist but is not shared transparently and proactively on LEA websites.

Leading Example

The Wisconsin Department of Public Instruction provides parents with a range of [resources](#) in understanding the agency’s legal obligations, including both Department-developed resources and links to 3rd party resources. They have clearly organized the information to be a step by step guide with options to learn more if interested.¹⁷

Finding #3: LEAs provide technology resources aimed at the devices they provide but privacy-specific resources are very rare.

Issues of technology, data and privacy can be mistakenly viewed as too complex for families, teachers, or other “non-technical” stakeholders.¹⁸ Yet, it is essential that LEAs support them in understanding these topics as it will support meaningful community engagement and ultimately increase trust in an organization more broadly.¹⁹ Moreover, there are risks to not engaging stakeholders in decision-making about data and technology. Specifically, organizations are more likely to encounter pushback on how data is being used if there is no buy-in on the front end, eventually limiting the effectiveness of data or the use of data.²⁰

Analysis of LEAs’ and SEAs’ websites and other publicly available information reveals areas of progress, as well as gaps in staffing and transparency:

Progress:

- Most LEAs devote section(s) of their websites to providing information directly to parents. Many provide guidance on using technology provided by the school to students, primarily devices (e.g. laptops, tablets).
- Some LEAs feature parent and teacher resources within the sections of their websites dedicated to technology use. The resources are often focused on devices provided by the school as well as remote learning, though a few include links to external resources that provide more comprehensive information about student privacy.

No LEAs provide a form or other mechanism that is specifically designated as a means for stakeholders to report student privacy concerns or related feedback.

Gaps:

- Very few LEAs provide resources related to student privacy for parents or teachers, although these were more prevalent on SEA websites. Resources that are available are most likely to be links to resources and training outside of the LEA.
- No LEAs provide a form or other mechanism that is specifically designated as a means for stakeholders to report student privacy concerns or related feedback.
- The vast majority of LEAs do not provide a list of edtech applications and software that are in use in schools, much less how the LEA is protecting information that is being shared with third parties. Relatedly, none of the LEAs publicly posts their data sharing agreements with third party providers.
- Although larger LEAs tend to have larger technology departments, they do not have greater transparency or resources regarding student privacy.

Leading Example

Denver Public Schools provides a series of extensive [training modules](#), required of all staff, on Student Data Privacy.²¹ These trainings are also available to the general public and easy to find on their website. They are also accompanied by a range of other resources, including a list of approved vendors, forms for approval of new vendors, and relevant policies.

Recommendations for Education Leaders

In addition to the bright spots uncovered by this research, it also shows that much work remains to improve staffing and transparency around student privacy. Specifically, SEA and LEA leaders can strengthen their efforts to realize the promise of increased use of edtech while ensuring students are kept safe online.

State Education Agency Actions

This research demonstrates that state guidance can influence LEA behavior. Given this, states should provide more guidance around best practices in transparency and staffing to support LEAs of all sizes. Furthermore, SEAs should offer support to LEAs on how to communicate their policies and practices to their stakeholders.

Additionally, because SEAs typically have more employees than LEAs do (and thus likely have more capacity related to privacy), they could consider developing resources for parents, teachers, and other stakeholders that LEAs could link to on their websites. This could include trainings, guidance, sample policies, and other resources. It could also include links to high quality resources developed by other nonprofit and advocacy organizations.

Finally, SEAs should consider creating opportunities for parents to provide feedback on privacy practices and policies and resources like training directed at parents or community engagement toolkits. SEAs could then share this feedback with LEAs, as well as create resources that incorporate this feedback that LEAs could then adapt to meet their communities' needs.

Local Education Agency Actions

In addition to the centralized support provided by state-level initiatives, LEAs can take steps to improve student privacy staffing and transparency. All LEAs experience resource constraints to some extent, but they must keep students safe and protect their privacy nonetheless. The following recommendations build on existing strengths within LEAs and can be adapted to fit the variety of LEAs' capacities. Additionally, when deciding on a path forward LEAs should

consider not only the resources needed to address issues of privacy but the risks of not implementing strong privacy policies and practices.

First, LEAs should designate and clearly communicate someone who is responsible for privacy, even if it is not the full scope of their role. Many LEAs distribute privacy duties across the organization. This can result in excessive data collection and access, untrained staff with little support protecting student data, retaining data past its usefulness, and lax controls on third party management and use of student data. Having a district staff member, ideally a senior level position, clearly responsible for issues of privacy can ensure appropriate attention is paid to these issues. It would also ensure that stakeholders know who to reach out to with questions or concerns.

Second, LEAs should make privacy information easier to find on websites for families, both through the standard navigation as well as the search function. This information could appear in a standalone website section, call out boxes in multiple places, or an alternative solution with appropriate language for parents and the public. The information provided should also be expanded to include not only the LEA's basic legal obligations, but more information on parents' rights and how families can exercise them, as well as additional information on how the LEA is going beyond bare legal compliance to protect student privacy. This could include at a minimum links to publicly available resources created by third party organizations aimed to help families understand their rights. LEAs could also consider developing their own, unique resources for families if they have capacity.

Additionally, LEAs should ensure they are engaging families and other stakeholders in issues of privacy. As a starting place, they can discuss these issues in existing forums for stakeholder engagement (such as a community committee, town halls, and surveys). A more robust form of engagement could include involvement of key stakeholders throughout the process of developing, implementing, and monitoring privacy policy and procedures.²²

Finally, LEAs may have policies and procedures in place around privacy but make them available only internally; the remaining step is to post them publicly. This includes documents such as the list of approved edtech applications, and links to external resources, such as parent webinars created by the SEA or affiliated nonprofits. Adapting and posting these policies and materials could increase transparency around student privacy efforts.

LEAs should ensure they are engaging families and other stakeholders in issues of privacy.



Conclusion

As the use of data and technology in education continues to evolve, it is important for states and LEAs to ensure they are taking appropriate steps to protect students' privacy online. They also should be proactive in dedicating staff and communicating with stakeholders about their procedures, both of which are important to protect student privacy.

Guaranteeing that families understand their rights, know a clear point of contact, and have training available will support meaningful community engagement, increase trust, and mitigate potential backlash, all of which are necessary to effectively use technology while protecting students.



Appendix: Methodology

State Selection

This research focuses on four states to understand the impact that state policies and procedures have on LEA behavior. States were selected based on the presence of student privacy laws and comparable geographies, sizes, and population demographics.

Sampling Methodology

Once states were selected, a random number generator selected 10 LEAs from each state based on LEA student enrollment and the percentage of economically disadvantaged students. The largest LEA in each state was included as a comparison (one of which was included in the original sampling of 40), resulting in 43 LEAs. CDT reviewed 14 LEAs with under 500 students, five LEAs with between 500 and 1,000 students, eight LEAs with between 1,000 and 2,000 students, three LEAs with between 2,000 and 5,000 students, seven LEAs between 5,000 and 10,000 students, and three LEAs above 10,000 students. In terms of students experiencing economic disadvantage, four LEAs had rates below 30%, 14 LEAs were between 30% and 50%, 13 were between 50% and 75%, and eight LEAs were above 75%.

Data Gathering

Because this research centers on transparency, the findings are based solely on publicly available information, specifically from LEA websites. Websites were accessed between May 25, 2022 and July 15, 2022. The information gathered included any attachments posted on the website (e.g., board meeting minutes, student handbooks, etc.) and was found using external search engines and those embedded within LEA websites.

Data Verification

The findings were shared with LEAs who were given the opportunity to provide factual corrections prior to publication; no corrections were received.



Endnotes


1. SC Media (2014, June 16) “*Human Error*” *Contributes to Nearly All Cyber Incidents, Study Finds*. Retrieved from: <https://www.scmagazine.com/home/security-news/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/>.
2. Elizabeth Laird, *Chief Privacy Officers: Who They Are & Why Education Leaders Need Them*, Center for Democracy & Technology (Jan. 2019), <https://cdt.org/insights/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them/>.
3. This includes the annual opt-out process for directory information, ability to access records, and limits on data sharing.
4. Hugh Grant-Chapman & Elizabeth Laird, *Key Views toward EdTech, School Data, and Student Privacy*, Center for Democracy & Technology (Nov. 2021) <https://cdt.org/wp-content/uploads/2021/11/CDT-Teacher-Parent-Student-Survey-Fall-2021-Final.pdf> [perma.cc/JBW7-G9X2].
5. Elizabeth Laird & Hannah Quay de-Valle, *Data Ethics and The Social Sector*, Center for Democracy & Technology (Feb. 2021), <https://cdt.org/insights/report-data-ethics-in-education-and-the-social-sector-what-does-it-mean-and-why-does-it-matter/>.
6. Local Education Agencies (LEAs) are the public authorities responsible for K-12 education in a particular geography, typically school districts or charter management organizations.
7. Elizabeth Laird, *Chief Privacy Officers: Who They Are & Why Education Leaders Need Them*.
8. Hugh Grant-Chapman & Elizabeth Laird, *Key Views toward EdTech, School Data, and Student Privacy*.
9. Elizabeth Laird, *Chief Privacy Officers: Who They Are & Why Education Leaders Need Them*.
10. It is likely that some staff are working on student privacy at least part-time, given legal requirements, but it is not apparent who these individuals are, making it difficult to know how LEAs are staffing student privacy and to whom the public should address questions and concerns.
11. https://www.oneidacsd.org/resources/staff_resources/data_privacy.
12. Hugh Grant-Chapman & Elizabeth Laird, *Key Views toward EdTech, School Data, and Student Privacy*.
13. Learn more at: <https://studentprivacy.ed.gov/resources/model-notice-directory-information>.
14. Learn more at: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA_Year1-3_CombinedReport%20Summary_Final.pdf.
15. See this model language at: <https://studentprivacy.ed.gov/annual-notice>.
16. Elizabeth Laird & Hannah Quay de-Valle, *Data Ethics and The Social Sector*.
17. <https://dpi.wi.gov/wise/data-privacy/parent-checklist>.
18. Elizabeth Laird & Hugh Grant-Chapman, *Sharing Student Data Across Public Sectors*, Center for Democracy & Technology (Dec. 2021) <https://cdt.org/insights/report-sharing-student-data-across-public-sectors-importance-of-community-engagement-to-support-responsible-and-equitable-use/> [perma.cc/HE8H-9WW8].
19. Ibid.
20. Elizabeth Laird and Hannah Quay de-Valle, *Data Ethics and The Social Sector*.


Endnotes

21. <https://www.dpsk12.org/student-data-privacy/>.
22. Elizabeth Laird, *Responsible Use of Data and Technology in Education: Community Engagement to Ensure Students and Families Are Helped, Not Hurt*, Center for Democracy & Technology (Feb. 2021), <https://cdt.org/insights/responsible-use-of-data-and-technology-in-education-community-engagement-to-ensure-students-and-families-are-helped-not-hurt/>.

 cdt.org

 cdt.org/contact

 Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

 202-637-9800

 @CenDemTech