OFFICE OF
Educational Technology

K-12 Digital Infrastructure Brief: Privacy Enhancing, Interoperable, and Useful

AUGUST 2023
U.S. DEPARTMENT OF EDUCATION
https://tech.ed.gov

August 2023

Version 1.0

Examples Are Not Endorsements

This document contains examples and resource materials that are provided for the user's convenience. The inclusion of non-Federal resources in this document is not intended to reflect its importance, nor is it intended to endorse any views expressed, initiatives, or products or services offered. Any opinions expressed in these materials do not necessarily reflect the positions or policies of the U.S. Department of Education or the Federal government. The U.S. Department of Education does not control or guarantee the accuracy, relevance, timeliness, or completeness of any outside information included in these materials.

Licensing and Availability

This report is available on the Department's Website at http://tech.ed.gov.

Requests for alternate format documents such as Braille or large print should be submitted to the Alternate Format Center by calling 1-202-260-0852 or by contacting the 504 coordinator via email at om_eeos@ed.gov.

Notice to Limited English Proficient Persons

If you have difficulty understanding English, you may request language assistance services for Department information that is available to the public. These language assistance services are available free of charge. If you need more information about interpretation or translation services, please call
1-800-USA-LEARN (1- 800-872-5327) (TTY: 1-800-437-0833) or email us at: Ed.Language.Assistance@ed.gov. Or write to: U.S. Department of Education, Information Resource Center, LBJ Education Building, 400 Maryland Ave. SW, Washington, DC 20202.

Contents

Acknowledgments

Project Team
The 2023 K-12 Digital Infrastructure Brief was published by the U.S. Department of Education, Office of Educational Technology (OET).

Michael Klein served as the principal lead in developing the brief with support from **Zac Chase**. Within OET **Bernadette Adams, Jessica Ch'ng, Yenda Prado, Ellery Robinson,** and **Ji Soo Song** provided technical assistance, under the guidance of **Kristina Ishmael** and **Roberto Rodriguez**.

Additional 2023 K-12 Digital Infrastructure Brief support was provided by the following K-12 Chief Technology Officers and other subject matter experts: **Douglas Alexander** (OSHEAN), **Valarie Byrd** (South Carolina Department of Education), **Doug Casey** (CCET, Connecticut Commission on Educational Technology), **Jennifer Covington** (Murray City School District), **Christine Fox** (CAST), **Ryan Kocsondy** (CEN, Connecticut Education Network), **Kim Lewis** (CENIC), **Amy Lewis Land** (Town of New Shoreham), **Mary McCarvel-O'Connor** (North Dakota Department of Public Instruction), **Pam McLeod** (Concord School District), **Joshua Olstad** (Oyster River Cooperative School District), **Kristi Peak-Oliveira** (Easterseals Massachusetts), **Sean Osborne** (South Carolina Department of Education), **Steve Smith** (A4L, Access 4 Learning), and **Darrell Williams** (Wisconsin Department of Public Instruction).

The following individuals provided additional assistance and support of the 2023 K-12 Digital Infrastructure Brief: **Susan Bearden** (InnovateEDU), **Lindsay Burton** (CISA), **Alaina Clark** (CISA), **Julia Fallon** (SETDA, The State Education Technology Directors Association), **Arlene Guevara-Zuleta** (CISA), **Kevin Herms** (U.S. Department of Education), **Angela Hernandez** (U.S. Department of Education), **Keith Krueger** (CoSN, The Consortium for School Networking), **Doug Levin** (K12 SIX, the K12 Security Information eXchange), **Amy McLaughlin** (CoSN), **Seeyew Mo** (ONCD, Office of the National Cyber Director), **Erin Mote** (InnovateEDU), **Ruth Ryder** (U.S. Department of Education), **Ryan Streeter** (CISA), **Valerie Truesdale** (AASA, the School Superintendents Association), **Mark Washington** (U.S. Department of Education), and **Bryan Williams** (U.S. Department of Education).

Introduction & Overview

This is the third in a series of five briefs[1] published by the U.S. Department of Education Office of Educational Technology on the key considerations facing educational leaders as they work to build and sustain core digital infrastructure for learning. These briefs offer recommendations to complement the fundamental infrastructure considerations outlined in the 2017 update to *Building Technology Infrastructure for Learning*. They are meant to provoke conversations, challenge conventions, and deepen understanding. These briefs have been purposefully designed to be easily consumed and shared.

The needs, capabilities, and expectations of technology infrastructure vary significantly by context. A rural outdoor learning school in the mountainous American Southwest will face challenges and have needs much different than a district within an urban center along the East Coast with an all-digital curriculum. The recommendations within these briefs are meant to help build, augment, and sustain digital infrastructure supportive of learning no matter the location.

America has made incredible progress in closing the digital access divide,[2] providing an ever-greater proportion of students with access to broadband connectivity, devices, and digital resources. At the same time, we must acknowledge the last frontiers of connectivity can also present the most wicked problems[3] of closing that divide. To help readers build solutions for their own contexts, these briefs offer examples from the field of those who faced pernicious challenges to connectivity, accessibility, cybersecurity, data privacy, and other infrastructure issues and designed solutions for their challenges. More examples can also be found at tech.ed.gov/stories.

Education Infrastructure is Critical Infrastructure

Education's digital infrastructure is officially considered critical infrastructure,[4] and just as we work to provide physical infrastructure that is safe, healthy, and supportive for all students, we need to align resources to create digital infrastructure that is safe, accessible, resilient, sustainable, and future-proof. Digital infrastructure includes "the resources that make digital

[1] The inclusion of non-Federal resources in this document is not intended to reflect its importance, nor is it intended to endorse any views expressed, initiatives, or products or services offered. Any opinions expressed in these materials do not necessarily reflect the positions or policies of the U.S. Department of Education or the Federal government. The U.S. Department of Education does not control or guarantee the accuracy, relevance, timeliness, or completeness of any outside information included in these materials.

[2] https://www.gao.gov/blog/closing-digital-divide-millions-americans-without-broadband

[3] https://www.stonybrook.edu/commcms/wicked-problem/about/What-is-a-wicked-problem

[4] The Education Facilities Subsector (EFS) within Government Facilities Sector was established with ED identified as the corresponding Sector Specific Agency (SSA) in the 2006 National Infrastructure Protection Plan (NIPP). The designation of EFS as "critical infrastructure" and ED's role as the agency responsible for the EFS has been reaffirmed in the 2009 NIPP, 2013 NIPP, Presidential Policy Directive 21, and, most recently, in Section 9002 of the Fiscal Year 2021 National Defense Authorization Act (NDAA). The 2021 NDAA renamed SSAs as Sector Risk Management Agencies (SRMAs) and articulated specific SRMA responsibilities. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources

systems possible and how individuals and organizations access and use these resources."[5] This considers the complex interplay of people, processes, and tools, including elements such as connectivity, security, interoperability, accessibility, affordability, and digital literacy as well as "behavioral, social, and physical barriers and opportunities for equitable adoption—who uses and does not use digital technologies and why."[6]

What Are We Working Toward?

To understand this imperative, consider the following hypothetical scenario, outlining one of many possibilities when digital infrastructure is operating optimally.

A Guiding Scenario[7]

A middle school principal opens a pre-meeting of school personnel who are part of the multidisciplinary team for an upcoming Individualized Education Program (IEP) meeting to discuss any anticipated revisions and opportunities for additional services. The case manager starts by pulling up a school-wide dashboard showing trends in the school's academic, attendance, and wellness data and showing how the student's data aligns with schoolwide data.

As the team navigates the student profile—a dashboard with the student's picture, grades, attendance, interests, and IEP goals—a special educator points out that the student has made progress on math goals but has continued to struggle with reading comprehension.

The Speech Language Pathologist (SLP) proposes that the student be considered for assistive technology (AT) services, which would include an evaluation of the student to determine whether and what AT could aid in addressing current learning needs. The proposal would include the ability for staff to safely collect the data they need to monitor the intervention's effectiveness and securely share the data with other systems like the student profile the team is currently reviewing. The Assistant Principal (AP) notes that in order to ensure that the AT evaluation also addresses the district's cybersecurity and data privacy requirements, the process would need to include input from the district's IT personnel. The AP asks the SLP to proceed with exploring this option, coordinate with IT staff, and copy the AP on emails to ensure that the various departments-special education, procurement, and IT continue to coordinate.

One of the student's general education teachers at the meeting notes the student's family is part of the district's affordable connectivity partnership with local internet providers and volunteers to include as part of the AT service proposal, a series of virtual meetings with the student and their family to demonstrate how to use the technology at home. The teacher, seeing a note on the dashboard that one of the student's parents is

[5] Borrowing from the United States Agency for International Development's definition in their August 2022 Digital Ecosystem Framework: https://www.usaid.gov/sites/default/files/2022-05/Digital_Strategy_Digital_Ecosystem_Final.pdf

[6] https://www.usaid.gov/sites/default/files/2022-05/Digital_Strategy_Digital_Ecosystem_Final.pdf

[7] It is important to note that personally identifiable data, information, and the education records of a student with a disability must be protected consistent with the Family Educational Rights and Privacy Act (FERPA) and the confidentiality protections of the Individuals with Disabilities Education Act (IDEA).

deaf, writes a reminder to re-familiarize himself with the contracted interpreter services and closed captioning function of the district's virtual conferencing platform. By taking these steps, the team ensures that the technology that best meets the student's needs also works with existing district tools and keeps the network secure prior to inclusion within the student's IEP.

The scenario above demonstrates the safe, effective, and helpful use of technology in support of learning and highlights the interplay of tools and processes, as well as the individual and organizational capacity that enables the use of technology to support students. Such scenarios rely on the following key tenets of digital infrastructure, which also guide the organization of this resource:

1. **Digital infrastructure should be adequate and future-proof.** Connections, speeds, and devices should be designed to meet the needs of modern education with plans for financial sustainability. This infrastructure should also be scalable to meet future needs.
2. **Digital infrastructure should be defensible and resilient.** Cybersecurity risk presents both a management and technical challenge. Ensuring the safety of people, data, and systems requires continuously building capacity to mitigate and respond to current risks like ransomware, as well as evolving cyber threats.
3. **Digital infrastructure should be privacy-enhancing, interoperable, and useful.** By prioritizing privacy and ensuring data protection measures, schools build trust with stakeholders and maintain the confidentiality and integrity of sensitive student data. Embracing interoperability standards can enable the seamless exchange of data between systems, empowering educators to make informed decisions and personalize learning experiences. Adherence to interoperability and privacy standards should be required from any third-party vendor or developer considered for inclusion within that infrastructure. Furthermore, personal data connected with users should be portable, allowing authorized users to take it with them and share it within and between educational systems.
4. **Digital infrastructure should be accessible to individuals with disabilities and multilingual learners.** Schools must provide equal access to individuals with disabilities. Planning for accessibility at all stages of the technology lifecycle—procurement, implementation, training, and support—as well as ensuring alignment to key accessibility-related frameworks and guidelines helps ensure that a school's digital infrastructure is readily accessible to individuals with disabilities. Schools must also take reasonable steps to ensure meaningful access to their programs and activities to people with limited English proficiency, which may include the use of multilingual digital content.
5. **Digital infrastructure should enhance student digital health, safety, and citizenship skills.** Digital infrastructure should be designed to protect and improve the digital health, safety, and citizenship[8] skills of the people within that system, including

[8] Digital citizenship is appropriate, responsible behavior when using technology, including social media, websites, online forums, communities, comments, and apps and other device features. Teaching children and teens digital

the privacy of their data. The existence and expansion of all such infrastructure should include clear plans for how to educate the end users and custodians of those systems in building and maintaining digital health, safety, and citizenship skills.

Whose Job Is It?

Building and maintaining safe, accessible, resilient, and effective digital infrastructure is a whole-of-community challenge requiring whole-of-community solutions. While every person has a role to play, the following groups play key roles:

- **District Leaders**: As organizational leaders, superintendents and senior district leaders play an important role in prioritizing secure digital infrastructure across the district and owning cyber risk management and digital accessibility at the executive leadership level. Put differently, if someone needs to announce a closure due to a cyberattack or answer questions from the board or press, it is likely to be the superintendent. To proactively address those risks, district leaders can focus the time, attention, and resources of students, staff, and leadership on practices that support secure, privacy-enhancing, accessible, and interoperable digital infrastructure.
- **District Technology Leaders**: As the primary implementers and maintainers of a district's digital infrastructure, chief technology officers and IT directors are often responsible for carrying out key aspects of mitigating cyber risk and supporting powerful teaching and learning for all students and staff. Technology leaders can create a culture of trust and security awareness by building processes for collaboration and coordination with students, staff, leadership, and outside experts. Technology leaders can also create the conditions for accessibility for all users by working closely with vendors during the design and procurement stages, and, when feasible, including individuals with disabilities in those processes.
- **Educators**: As the group tasked with facilitating high-quality teaching and learning to all students, educators (including general educators, special educators, related service providers, paraprofessionals, and others) often see the greatest possibilities and most frustrating constraints when it comes to digital infrastructure. As those often closest to the educational and social-emotional needs of students, educators seek out the most effective tools to meet their students' needs. They can have a powerful impact by practicing essential cyber hygiene and modeling it for students and families. By collaborating with IT/technology professionals to consider cybersecurity, data privacy, and accessibility when reviewing digital tools, educators can help to ensure all students have access to safe, secure, accessible, and powerful learning experiences.
- **Students and Families**: In partnership with schools and communities, families can collaborate with teachers and support secure access to digital infrastructure at home. Feedback from students and families can be an important way for schools to understand when tools or experiences are inaccessible, when data in progress reports are confusing, or when they feel unsafe in school or online. Students and families can also advocate that districts and vendors protect the privacy of students' data. For more on student

citizenship skills can help prevent cyberbullying and its negative effects. When children learn positive online behaviors, social media can be used in productive ways. (source: Digital Citizenship Skills | StopBullying.gov)

data privacy and federal laws see *K-12 Digital Infrastructure Brief: Privacy-enhancing, Interoperable, and Useful*.

- **State Leaders**: State educational agency (SEA) leaders help support educational technology (edtech) infrastructure by modeling institutional best practices, developing thoughtful policy and guidance, and providing adequate resourcing to support policy implementation. For example, SEA staff may leverage the Office of EdTech's 2023 Dear Colleague Letter to help districts plan for and use their federal education funds to support digital equity, including hiring instructional coaches and providing professional learning for educators.
- **Vendors and Service Providers**: Vendors and service providers play an outsized role in the privacy, security, accessibility, and interoperability of K-12 digital infrastructure. The K-12 education sector's reliance on third-party providers includes costs and benefits. While each vendor and service provider adds supply chain risks that can be opaque and challenging to mitigate, these providers often provide services districts cannot support and maintain on their own, such as secure backups and cloud storage, as well as web templates, electronic portals, and applications. In addition, some vendors invest substantial resources in cybersecurity and data privacy (often more than a district could afford on its own). Finally, improvements in the security posture or digital accessibility of a vendor or service provider used widely in K-12 can benefit thousands of school districts, rather than needing to fix vulnerabilities or accessibility barriers district by district.

And many more: Within school districts, district and school staff interact regularly with sensitive student and staff data, while district leaders in special education, finance, human resources, operations, and curriculum play important roles in managing risk and ensuring accessibility. Educational service agencies (ESAs) often help build the capacity of thousands of school districts across the country, sometimes by managing a district's entire digital infrastructure. Federal partners like the U.S. Department of Education (ED),[9] Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and others play a critical role in providing technical assistance, sharing intelligence and analysis, and investigating criminal cyber activity, while the Federal Communications Commission provides vital funding via the E-Rate program.

Key Considerations

Key considerations within this brief include:

Privacy: Ensure that student data is protected and that policies are in place to address data collection, storage, usage, and access.

Interoperability: Implement data interoperability standards to allow the seamless exchange of data between different edtech applications and systems.

[9] ED has limited authorities related to K-12 cybersecurity. The 2013 National Infrastructure Protection Plan (NIPP) and the FY21 National Defense Authorization Act (NDAA) designated ED as the Education Facilities Subsector (EFS) Sector Risk Management Agency (SRMA). Within current authorities, ED can provide technical assistance related to K-12 cybersecurity.

Usefulness: Build data systems and digital infrastructure that provide useful and actionable information to educators, administrators, and other stakeholders for decision-making and improving student outcomes.

Compliance with federal and state privacy laws: Learn and adhere to relevant federal privacy laws such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), Individuals with Disabilities Education Act (IDEA), Children's Internet Protection Act (CIPA), Protection of Pupil Rights Amendment (PPRA), and Health Insurance Portability and Accountability Act (HIPAA), as well as state laws to protect student privacy rights.

Data equity and visualization: Apply an equity lens to data practices, ensuring that data is collected and analyzed in a way that addresses historic and systemic bias. Utilize data visualization tools to communicate data effectively and promote understanding among stakeholders.

Digital Infrastructure Should be Privacy-Enhancing, Interoperable & Useful

We Were Promised Flying Cars

Technology has always held the promise of transforming teaching, learning, and operations. In one version of imagined futures, learners would access the perfect progression of learning experiences for them at exactly the right time. Educators would provide targeted support to flexible groups of students based on reliable real-time data, while technology would automate the mundane tasks that consume teacher time and attention. District leaders would ensure every student had the academic and social emotional supports in place to thrive in school and pursue the career pathway of their choosing, while efficiently and effectively stewarding the district's financial and human capital resources.

For many districts, the future described above can feel as unattainable as a flying car. However, districts across the country can take action with concrete steps to ensure their digital infrastructure—specifically their data infrastructure—can improve teaching, learning, and operations today. By building data systems and digital infrastructure that are interoperable, portable, privacy-enhancing, and user-centered, schools can ensure data are useful for all users as they make meaning, make decisions, and make a difference.

Making Data Useful Now

In the guiding scenario from the introduction, each educator on the team had access to the data they needed to inform their decisions about which students need support and which interventions to implement. The team achieves this with a tool that pulls together data from relevant district data sources in real-time and visualizes the most important elements at the school, class, group, and student level. Given the sensitive nature of the data, including IEPs and behavior data, each member is given role-based access that allows them to see only the students and data they need for their role in supporting the students' needs. This is not a flying car. This kind of system is attainable today, and to get there starts with student data privacy.

Privacy Enhancing: Keeping Data Protected

Those responsible for safeguarding student data must be mindful of and transparent about how data privacy, confidentiality, and security practices affect students. Schools and districts should develop policies that allow them to provide students and families with answers to questions such as:

- What types of student data does the school or third parties acting on its behalf (e.g., edtech tools) collect?
- How is the data stored?
- How can the data be used?
- Who has access to student data? For which students? For which purposes? For how long?
- What are families' and students' rights and responsibilities concerning data collection?

Additionally, vendors would do well to anticipate these questions and offer transparent responses on their websites and promotional materials. The Department's student privacy website offers this resource for "Developing a Privacy Policy for Your District."

While many districts have data security and transparency policies for formally adopted digital resources, many fail to adequately address the issue of click-wrap agreements. Click-wrap agreements appear when users are asked to accept the provider's terms of service before using a website or software application. Click-wrap agreements enter the developer and the user (in this case, the school or district) into a contractual relationship akin to signing a contract. Often, user agreements are entered into by classroom teachers who have had no training on the impact or implications of user agreements, nor knowledge of relevant federal, state, or district policies that protect student data privacy. To address this need, districts should incorporate training on this issue into new-teacher orientation and provide additional professional development on a regular basis, in the same way educators engage in emergency medical training. The "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" document offers some specific practices to help educators better navigate click-wrap agreements.

Federal Privacy Laws and K-12 Education

The **Family Educational Rights and Privacy Act (FERPA)** gives parents and "eligible students" (i.e., students who are 18 years of age or attending an institution of postsecondary education) the right to exercise some control over the disclosure of, to inspect and review, and to seek to amend student education records maintained by educational agencies (e.g., school districts) or institutions (i.e., schools). For example, under FERPA, an educational agency or institution may generally only disclose education records, or personally identifiable information (PII) contained therein, with the prior written consent of a parent or an eligible student.

There are a few exceptions to FERPA's general written consent requirement. One such exception permits an educational agency or institution to disclose, without consent, student education records, or PII contained therein, to contractors, consultants, volunteers, or other third parties to whom the educational agency or institution has outsourced institutional services or functions, provided the third party constitutes a school official with a legitimate educational interest under the criteria listed in the educational agency's or institution's annual notification of FERPA rights; performs an institutional service or function for which the educational agency or institution would otherwise use employees; is under the direct control of the educational agency or institution with respect to the use and maintenance of the education records; and is subject to the FERPA requirements governing the use and redisclosure of PII from education records in 34 CFR 99.33(a). (For more information on FERPA, visit the Department's Student Privacy website, https://studentprivacy.ed.gov/.)

The **Children's Online Privacy Protection Act (COPPA)** governs online collection of personal information from children under 13 years of age. Before a commercial website or online service directed towards children can collect any information from students under 13, "verifiable parental consent" is required. The Federal Trade Commission (FTC), which enforces COPPA, has said that school officials can, in certain situations, provide consent on behalf of the parents as long as that consent is limited to the educational context—where an operator

collects personal information from students for the use and benefit of the school for no other commercial purpose. (For more information on COPPA, please visit the FTC's COPPA FAQ website.)

The **Individuals with Disabilities Education Act (IDEA)** includes confidentiality requirements to protect the privacy interests of children with disabilities from birth until age 21 who are referred for services under IDEA. IDEA protects PII in the education records of those children. IDEA generally requires that a parent provide prior written consent before PII is disclosed to a third party and that the parental consent must be informed. There are some specific exceptions that may apply to the general rule of parental consent.

The **Children's Internet Protection Act (CIPA)** imposes several requirements on schools or libraries that receive E-Rate discounts for internet access. Schools and libraries must certify that they have technologies in place to block or filter internet access to content that is obscene, pornographic, or harmful to minors, and schools must also monitor the online activities of minors. The FCC's CIPA Guide offers a more in-depth understanding of CIPA requirements.

The **Protection of Pupil Rights Amendment (PPRA)** provides parents of students certain rights regarding, among other things, participation in surveys and the collection and use of information for marketing purposes. (These rights transfer from a parent to a student when the student turns 18 years old or becomes an emancipated minor under applicable state law.) This includes, but is not limited to, the right to receive direct notice and an opportunity to opt a student out of activities of a local educational agency (LEA) involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose), with some exceptions. LEAs must make this notification to parents at least annually at the beginning of the school year and must include the specific or approximate dates during the school year when the activities are scheduled or expected to be scheduled. For activities that are scheduled after the school year starts, LEAs must provide parents with reasonable notification and an opportunity to opt their child out. This notice and opt-out right does not, however, apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions. Parents also have the right to inspect, upon request, any instrument used by an LEA to collect personal information for the purpose of marketing or sale (or otherwise providing that information to others for that purpose) before the instrument is administered or distributed to a student, with some exceptions. (For more information regarding PPRA, see the Department's PPRA General Guidance document.)

The **Health Insurance Portability and Accountability Act (HIPAA)** sets national standards for the privacy of protected health information (PHI) and security of electronic PHI. The HIPAA Privacy Rule does not apply to records that are protected by FERPA, but other aspects of HIPAA may apply to covered entities, such as if they are conducting electronic billing of PHI in health-related claims. For a better understanding of the issue, see the jointly published guidance from the U.S. Department of Health and Human Services and the U.S. Department of Education.

Technical Assistance Resources at the U.S. Department of Education

The Student Privacy Policy Office (SPPO)'s Privacy Technical Assistance Center (PTAC) is a one-stop resource to learn about privacy related to student data. Through the PTAC, SPPO provides information on privacy, confidentiality, and security practices via training materials, direct technical assistance, and recommendations on Protecting Student Privacy while Using Online Educational Services and Transparency Best Practices for Schools and Districts.

Another valuable resource, the Data Breach Scenario, is intended to assist schools, districts, and other educational organizations with internal data security training. The Password Data Breach interactive exercise is aimed at district management and provides a simulated response to a district-level data breach that focuses on the processes, procedures, and skills needed to respond.[10]

Student Data Privacy Consortium (SDPC)

Founded in 2015, the Student Data Privacy Consortium (SDPC) is a collaborative of SEAs, ESAs, LEAs, vendors, and policymakers "addressing real-world, adaptable, and implementable solutions to growing data privacy concerns [focusing specifically] on those issues being faced by "on-the-ground" practitioners."[11] Since SDPC launched the SDPC Resource Registry in 2016 to help members manage their data privacy agreements, the community has added 9,061 resources and 96,818 signed Data Privacy Agreements. Building on that success, the SDPC community—which includes 36 participating states (24 active alliances) representing 11,361 school districts—developed the National Data Privacy Agreement (NDPA) to streamline procurement and "set common expectations" around student data privacy for districts and vendors. In addition to providing a common baseline for student data privacy protections, NDPA includes the option for states to add "Supplemental State Terms," developed by SDPC-affiliated state alliances, to account for state-specific privacy legislation.

NH Builds Statewide Expectations & Support for Student Privacy

Concord School District Technology Director Pamela McLeod co-founded the New Hampshire Student Privacy Alliance (NHSPA)[12] in 2019 with Oyster River Technology Director Joshua Olstad, in response to New Hampshire's House Bill 1612.[13] The House Bill required all schools in that state to create a data governance plan and hold their vendors accountable to a set of NIST-derived information security standards. By joining together and paying a fee of $1.10 per student, the 82 school districts in NHSPA pay for a consultant to negotiate with the vendors, providing the districts greater leverage over the vendors than if they "go-it-alone" and reducing the workload for each district. Since 2019, NHSPA has entered into a shared data privacy agreement template with 4 other New England states and has "successfully entered into data privacy agreements with over 1,300 products."[14] According to McLeod, the NHSPA is having a powerful impact for district technology leaders: "When we sign the contract, we know that our

[10] https://studentprivacy.ed.gov/resources/data-breach-response-training-kit
[11] https://privacy.a4l.org/privacy-community/
[12] NHSPA is a project under the umbrella of the NH CTO Council, the state CoSN affiliate organization.
[13] https://www.education.nh.gov/who-we-are/division-of-educator-and-analytic-resources/bureau-of-education-statistics/data-governance
[14] https://www.concordmonitor.com/how-schools-manage-student-data-privacy-in-NH-48674676

liability has been transferred from us to the company…It's also kind of shifting the heavy lifting to the districts which have more staff and more capabilities, and kind of letting the smaller districts pay a little bit less attention."[15]

Data Interoperability: Putting Data to Work

Securing student data only takes schools and districts so far. Almost every U.S. school district faces the same core challenge when it comes to leveraging data to spark innovation and improve student outcomes: they can't effectively use the information they've already collected. One major driving force behind this data usability challenge is that school data currently lives in hundreds, if not thousands, of disparate tools that store the data in different formats and may not allow that information to be easily accessed or exchanged with other systems. Since 2016, Project Unicorn—a coalition of concerned organizations including education non-profits, charitable foundations, school districts, and industry partners—has been working to solve this thorny problem through the adoption of data interoperability standards across edtech. According to Project Unicorn, "interoperability is the **seamless**, **secure**, and **controlled** exchange of data between applications. At the core of interoperability is a focus on better informing instruction and driving student-centered learning experiences."[16] Exploring state and district interoperability implementations shows how organizations leverage this powerful approach in practice.

Saving Time and Money in Wisconsin's SEA

The Wisconsin Department of Public Instruction (DPI) provides a powerful example of how an SEA can collaborate with LEAs, nonprofit organizations, and vendors to implement data systems that save time and money while dramatically improving data quality and operational efficiency. In 2016, DPI introduced the Wisconsin Information System for Education Data System (WISEdata) Ed-Fi Integration Project[17] "to improve the collection of required state and federal data and replace individual legacy collection systems…with a cohesive interoperability collection framework."[18] Following the success of this project, in 2020, DPI implemented WISEdata Finance to build upon the model and collect financial data. By requiring student information system, financial data system, and other technology providers to implement the Ed-Fi interoperability framework, DPI enables LEAs to easily push data to DPI from their vendors' systems through an application programming interface (API). This data is then used by DPI teams responsible for monitoring federal programs and allows for automated messages to LEAs when budgets dip below compliance standards allowing them to reconcile financial accounts in real-time. To make the process easy for LEAs and vendors, DPI provides a Certified Vendor List, a New Vendor Application form, and a comprehensive Vendor Onboarding Process on the DPI website. Building on these successes, DPI has further leveraged these collections to help LEAs ensure that accurate student immunization records meet school immunization requirements. By

[15] https://www.concordmonitor.com/how-schools-manage-student-data-privacy-in-NH-48674676
[16] https://www.projectunicorn.org/what-is-interoperability
[17] "The Ed-Fi Alliance is a non-profit initiative that creates and maintains the Ed-Fi data standard and technology suite to enable education agencies to have a real-time, comprehensive view of their data so they can solve entrenched challenges at scale." https://www.ed-fi.org/blog/success_stories/wisedata-from-broken-budgets-to-real-time-reconciliation/
[18] https://dpi.wi.gov/wisedata/ed-fi-integration

retrieving student immunization records from the Wisconsin Department of Health Services and passing it back to the LEAs through their SIS, DPI's Ed-Fi integration provides cost savings to LEAs in terms of staff time and allows for better management of vaccination records.[19]

What Vendors Can Do

- FTC's Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business: Vendors can take specific actions outlined in this guidance to ensure their practices align with COPPA requirements.
- Project Unicorn Interoperability Rubric: Vendors can use the rubric as a self-assessment to determine the maturity level of their product and set goals for improvement. States and districts can use the interoperability rubric to evaluate vendors and inform language in their Requests for Proposals (RFP).
- Project Unicorn Edtech Vendor Pledge: Vendors can pledge their "commitment to increase secure access, privacy, and interoperability in your products and empower customers, educators and families to achieve an enhanced level of engagement in their students' education to improve the impact of educational data and to inform teaching and learning practices for stronger student outcomes." By signing the pledge, vendors get access to the Interoperability Certification application at no cost.
- Project Unicorn Interoperability Certification: Vendors can seek this certification to signal to school districts that their product prioritizes interoperability.

Usefulness: Helping Data Tell Stories

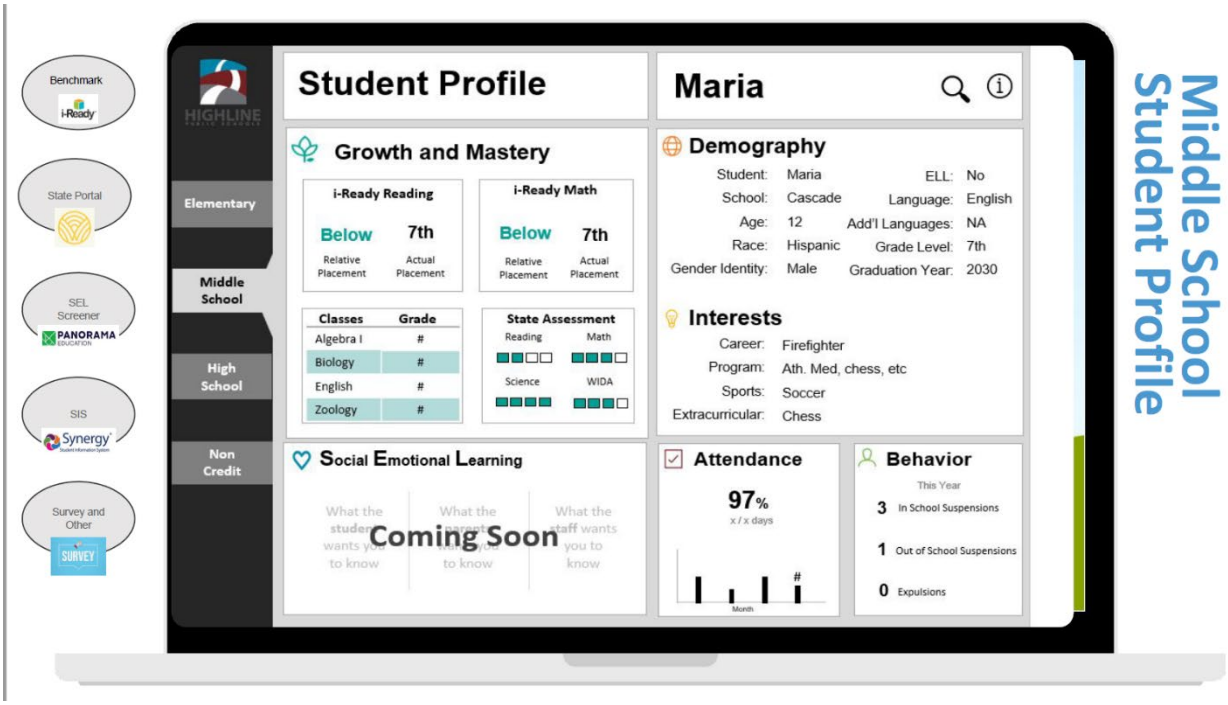
While data interoperability can unlock a more holistic view of students, districts in the Digital Promise Data Equity cohort are going a step further by "applying an equity lens and mindset to the ways in which districts collect, analyze, interpret, communicate, and make decisions based on data, with the goals of acknowledging and addressing historic and systemic bias and building more equitable policies, practices, and systems."[20] To help districts leverage data interoperability for equity and inclusion, Digital Promise created the Data Ready Playbook. The playbook is built on a Readiness Framework that incorporates three domains—project governance, needs assessment, and implementation plan—and guides districts through activities, use cases, and resources that culminate in a data equity project plan and slideshow for pitching the project. The process builds organizational capacity and readiness for equity-informed data interoperability work.

One District Visualizes Student Success

In Washington's Highline Public Schools, the district promises that every student "is known by name, strength, and need and graduates prepared for the future they choose."[21] For Dr. Rebekah Kim, Executive Director of Teaching, Learning, and Leadership in Highline, delivering on that promise started with a simple yet profound question: "What would a strengths-based

[19] https://www.ed-fi.org/webinar/wisconsin-ed-fi-streamlining-immunization-health-record-data-for-districts/
[20] https://digitalpromise.org/initiative/league-of-innovative-schools/data-ready-playbook/
[21] https://www.highlineschools.org/about/district-information

profile for teachers and students look like?"[22] That strengths-based profile combined with capacity building around data literacy would empower each stakeholder to answer the question, "Now what?" Dr. Kim knew all too well that –even with the shiniest, coolest state-of-the-art data analytics tools— unless educators and families knew what to do next based on the tool, there would be no transformative impact on teaching and learning. Through a combination of enduring leadership sponsorship, ongoing cross-departmental collaboration, and deep connection to the district's vision, the team at Highline has made tremendous progress toward an equity-focused student and staff profile. See an example of the student profile below (not a real student and no PII shown).



Data Portability

As districts leverage data interoperability and data equity to unlock the transformative potential of data to support students furthest from opportunity, leaders will need to engage with the risks and benefits related to data portability. According to the Center for Democracy and Technology (CDT) report Protecting Privacy While Supporting Students Who Change Schools, "Data portability is a technical term that refers to copying, downloading, exporting, or transferring data. In the case of student mobility, data portability refers to sharing data across schools when students are leaving one school to enroll in another."[23]

While data portability may sound technical or arcane, it can have a profound impact on "critical decisions that influence educational outcomes of a student," especially among highly mobile

[22] Project Unicorn 2021 State of the Sector Approach https://bloximages.newyork1.vip.townnews.com/fwbusiness.com/content/tncms/assets/v3/editorial/f/58/f58e7d54-d459-5e93-847c-9f0c8839ab9e/61f8bc7681b44.pdf.pdf

[23] https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf

student groups such as migratory students, students experiencing homelessness, students in foster care, students going in and out of incarceration, and military-connected students. For example, by providing student information to the right person at the right time, data portability can enable a student's new school to ensure timely enrollment, class placement, continuing IEP-related services, and keeping students safe from things like severe food allergies.[24]

It is also important to recognize and mitigate the potential harms that could come to the student from that data. Beyond the most obvious harm of a data breach (discussed in more detail below), CDT identifies three common privacy harms that require mitigation:[25]

- **Jeopardizing Physical Safety**: If a student has been placed in foster care to avoid an abusive parent and the new school does not have access to the student's records, the new school could unwittingly release the child to the abusive parent resulting in imminent danger and harm to the child.
- **Creating Social Stigma**: For a student experiencing homelessness, something as simple as a teacher asking where the student is currently living around other students can lead to bullying, harassment, and alienation.
- **Making Biased Decisions**: "Oversharing information, especially without context, can enable decision-making that disadvantages or discriminates against an individual student. Therefore, adopting an approach to **data minimization** (e.g., deleting data once it is no longer needed or limiting the amount of data initially collected) is critical."

Conclusion

Educational leaders have the power to drive meaningful change by prioritizing digital infrastructure that is privacy enhancing, interoperable, and useful. To make this vision a reality, they should take concrete steps to establish robust data governance policies, adhere to relevant privacy laws, and collaborate with SEAs, ESAs, LEAs, nonprofits, and vendors that are working toward the same goals. Leaders should seize the opportunity to advocate for data interoperability, promote data equity, and invest in data literacy training and expertise. Embracing these actions can shape an edtech landscape that truly supports teaching, learning, and improved outcomes for every student.

[24] https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf
[25] https://cdt.org/wp-content/uploads/2019/07/2019-06-20-Portability-and-Privacy-Issue-Brief.pdf