Infrastructure Modernization

**EDITOR’S NOTE**
Infrastructure modernization would transform American education. This Spotlight will help you grasp the reality of school infrastructure; understand parent privacy concerns with ed tech; be aware of privacy group warnings on tech that flags some children; review watchdog recommendations on decreasing cyberattacks; know the impact of broadband investments; understand an initiative to aid with tech purchasing; and avoid mistakes when spending COVID-relief funds.

---

*The Infrastructure Bill Includes Billions for Broadband. What It Would Mean for Students .......................... 2*

*Privacy Group Cautions Schools On Technology That Flags Children at Risk of Self-Harm .................. 3*

*Tech Purchasing Decisions Are Super Hard. New Initiative Aims to Help ........................................... 4*

*Cyberattacks Are Up. The Feds Must Help Schools Cope, Watchdog Agency Says ......................... 5*

*The Dismal State of School Infrastructure, in Charts ......................... 6*

*Ed Tech Usage is Up. So Are Parent Privacy Concerns .................. 7*

**OPINION**
5 Mistakes to Avoid When Spending COVID-Relief Funds ............ 8
The Infrastructure Bill Includes Billions for Broadband. What It Would Mean for Students

By Alyson Klein

Students and teachers who struggle to access the internet at home may get some relief from a sweeping, more than $1 trillion federal investment in infrastructure.

The package—which was approved by Congress Nov. 5 and is expected to be signed into law by President Joe Biden—includes nearly $65 billion to improve access to broadband and help the country respond to cyberattacks.

The funding is a good step forward in helping to close the so-called “homework gap,” or the difficulty millions of students—particularly poor, minority, and rural kids—have in getting online at home to complete school assignments, said Keith Krueger, the chief executive officer of the Consortium for School Networking, which supports K-12 education technology leaders.

“While there’s been a huge strategy by many school districts to provide hotspots [and get] connectivity to students who don’t have it, there are still large swaths of the country that are too rural or remote ...”

KEITH KRUEGER
Chief executive officer of the Consortium for School Networking

Even as school-issued devices such as Chromebooks, shown above, have proliferated in the pandemic, many students still lack internet access at home, putting them at a disadvantage for completing homework assignments.

The legislation also includes $2.75 billion for “digital equity,” designed in part to focus on aspects of connectivity beyond broadband expansion. That funding could go to a wide-range of expenses, anything from laptops for students to digital literacy classes for senior citizens at the local library, according to a statement from Sen. Patty Murray, D-Wash., who championed the program.

The money would be used in part to pay for two new grant programs, including $300 million in grants over five years to help states create and implement plans to improve digital equity. Another $250 million over five years would support individual groups’ and communities’ digital equity projects.

Still, it’s important to keep in mind that the homework gap may persist, even after more students have at least some broadband access at home, Krueger said. For instance, students may not have a connection strong enough to stream video lessons, or enough devices in their household to go around.

“The media headline has been about the unconnected, but the under connectivity is extremely important,” he said. “It isn’t just a matter of handing [kids] a hotspot or giving them a cheap device that can’t do video conferencing. We have to invest in robust tools.”

How will this bill help students with little or no connectivity at home?

The biggest chunk of the money—$42.5 billion in “broadband deployment grants”—is aimed at expanding broadband infrastructure to reach families and businesses in rural and other underserved areas. That may help students and teachers who have been unable to take full advantage of district-provided hotspots because the area they live in doesn’t have the kind of connectivity needed to operate them.

It also includes $14 billion to help low-income households connect to broadband. That could help students who live in connected areas but remain offline because their families can’t cover the cost of internet service.

That’s about two-thirds of the 28 million households that aren’t connected, or about 18 million families, according to a recent report from EducationSuperHighway, a non-profit that champions internet access.

While there’s been a huge strategy by many school districts to provide hotspots [and get] connectivity to students who don’t have it, there are still large swaths of the country that are too rural or remote ...

—Rich Pedroncelli/AP

Even as school-issued devices such as Chromebooks, shown above, have proliferated in the pandemic, many students still lack internet access at home, putting them at a disadvantage for completing homework assignments.
Growing, thanks in large measure to the COVID-19 pandemic, which forced more students online and sparked an apparent rise in student suicides and mental health crises. Popular ed-tech company Gaggle, for example, now claims 1,500 school district clients and counting.

"In a school setting—whether virtual or in person—adults have a legal obligation to keep kids safe," Gaggle CEO Jeff Patterson said in a statement. "Gaggle believes firmly in the importance of protecting student privacy and is a long-standing supporter of the Future of Privacy Forum’s Student Privacy Pledge 2020 and would welcome opportunities to continue to collaborate with FPF.”

Amelia Vance of the Future of Privacy Forum stopped short of saying K-12 leaders should forgo such systems altogether but warned educators to do extensive diligence before adopting them.

"Schools should not employ self-harm monitoring unless they have robust mental health resources established and common-sense data protections in place,” said Vance, the director of youth and education privacy for the group.

**Self-harm monitoring systems raise privacy, equity, legal concerns**

The new report describes self-harm monitoring systems as “computerized programs that can monitor students’ online activity on school-issued devices, school networks, and school accounts to identify whether students are at risk of dangerous mental health crises.”

Such systems typically collect and scan digital information ranging from students’ web-browsing histories to the contents of their documents and email messages, using algorithms and sometimes human reviewers to search for keywords that might indicate trouble. When content is flagged, alerts are typically sent to school or district administrators, who sometimes take the information to third parties such as law enforcement.

The companies who make such tools regularly tout hundreds or thousands of lives saved and catastrophes averted.

A Gaggle spokeswoman, for example, said in a statement that the company saved 1,408 lives last year alone. That number is based on either reports back from district clients and/or flagged content that contained a “clear and definitive” suicide plan. Gaggle is among the companies that uses trained human reviewers to determine which flagged content merits an alert to school officials.

Still, the Future of Privacy Forum suggests it’s unclear whether self-harm monitoring systems can accurately identify a high percentage of at-risk students while avoiding “false flags” of children who are not really considering harming themselves or others.

And even when self-harm monitoring systems do work as advertised, it’s not clear that merely flagging students’ digital content reliably leads to an appropriate mental health intervention.

The group’s new report also details a range of other potential problems:

- **Legal violations:** While schools are required by the Children’s Internet Protection Act to block obscene or harmful content on their networks and devices, it remains unclear whether the federal law clears the way for self-harm monitoring technologies as filters, the Future of Privacy Forum says. It’s also unclear how the Family Educational Rights and Privacy Act applies to the information such technologies gather on students, and surveilling and flagging students’ off-campus online activity may in some circumstances violate Fourth Amendment protections against unlawful searches and seizures.

- **Equity concerns:** Vulnerable children and students from “systematically marginalized groups” may face an
Tech Purchasing Decisions Are Super Hard. New Initiative Aims to Help

By Alyson Klein

District and school leaders are facing some of the most difficult and expensive technology purchasing decisions of their careers. But they are struggling with where to go to get objective information about ed-tech products.

The International Society for Technology in Education is trying to fill the void.

“It is very hard to get information about different products,” said Richard Culatta, the chief executive officer of ISTE. “Sure, companies will happily give you a whitepaper that says how great everything is, but it’s hard to get real, accurate information.”

Individual groups, he said, have attempted to create a sort of Consumer Reports for ed-tech products, but that’s been tricky and time-consuming to pull off.

So ISTE is working with partner organizations to build a national database of ed-tech products. It will be up to vendors to add their products to the list. And each product will be given a universal learning technology ID or UTID.

“It is imperative that school districts approach any self-harm monitoring system holistically, taking into account the totality of harms that could arise from hastily adopting technology without well-developed implementation policies and the necessary accompanying school-based mental health resources,” the report concludes.

GoGuardian, makers of widely used filtering and monitoring services now used by roughly 14,000 schools and districts nationwide, applauded the recommendations as “thoughtful.”

“We recognize the important role that school leaders play in balancing student privacy and safety in the digital age and are committed to building solutions that support that balance,” a company spokesman said in a statement.

Among those sharing such concerns is the National Association of School Psychologists, which has not taken an official position on whether schools should use self-harm monitoring technologies.

“We would raise cautions about the possibility of wrongly identifying students or misuse of data,” a spokeswoman for the group said via email.

Monitoring systems not a substitute for mental health services

NASP and the Future of Privacy Forum were also aligned in recommending that K-12 districts ensure they have an adequate number of school psychologists, counselors, and social workers to support the needs of students who are at risk.

“Monitoring systems cannot serve as a substitute for robust mental health supports provided in school or a comprehensive self-harm prevention strategy rooted in well-developed medical evidence,” the report says.

Other recommendations include working with parents and community members to develop a shared understanding of values and priorities before adopting monitoring technology; developing clear policies about what information is collected, who has access to it, and how long it is stored; and clearly communicating those policies to school staff and parents alike.

“We recognize the importance of ensuring that school districts have robust. monitoring systems in place that are consistent with best practices for student privacy,” said NASP President Julie Sweeting in a statement.

“Going forward, school districts must play a role in ensuring that monitoring systems are not being used as a substitute for robust mental health supports,” she said.

“Monitoring systems cannot serve as a substitute for robust mental health supports provided in school or a comprehensive self-harm prevention strategy rooted in well-developed medical evidence,” the report says.

Other recommendations include working with parents and community members to develop a shared understanding of values and priorities before adopting monitoring technology; developing clear policies about what information is collected, who has access to it, and how long it is stored; and clearly communicating those policies to school staff and parents alike.

By Alyson Klein
name of the product, a description, the grade or grades that the product is intended for, the topic it covers, and the pricing structure.

And soon, the database will be expanded to include other factors such as whether the products meet interoperability standards and feature privacy policies. Down the road, the hub may include information like research studies on a particular product or approach, and a way for educators to share their own experiences with the product.

Other organizations—such as Common Sense Media, a nonprofit that works on issues related to youth and technology, and Digital Promise, which works to improve innovation in K-12—are partnering with ISTE and could add some of their own information to the database.

The timing of this new database is really important, Culatta said, in part because districts have unprecedented amounts of money in federal COVID relief aid to spend on helping students and schools recover from the pandemic. Educators want to make sure they’re making good choices.

“We have billions and billions of dollars going out to school districts, right now, and they are telling us, we need help, making these decisions,” Culatta said. “For a digital education ecosystem, we’ve been in a shockingly analog world when it comes to how we make decisions about the products we buy. And our goal is to change that.”

Published November 17, 2021

Cyberattacks Are Up. The Feds Must Help Schools Cope, Watchdog Agency Says

By Alyson Klein

The U.S. Department of Education’s more-than-a-decade old plan to help protect schools from digital threats needs a rethink, as cyberattacks rise and new threats emerge, concludes the Government Accountability Office, Congress’ watchdog arm, in a report out this month.

Since 2010, when the plan was last updated, K-12 schools have dramatically ramped up their use of education technology, leaving their systems more vulnerable to threats. That’s been particularly true during the COVID-19 pandemic, which forced schools to switch over to online learning at lightning speed.

“The efforts that the schools had to go through last year to convert from in-person to virtual learning put a lot of strain and stress on the technology services that they either had or they needed to acquire very quickly,” said Nick Marinos, a director on the GAO’s Information Technology and Cybersecurity team in an interview with Watchdog Report, the GAO’s podcast. “In other cases where we’ve seen entities have to rush to put forward technology, cybersecurity often can be an afterthought or something that might not get attention until, unfortunately, an attack or an incident occurs.”

These attacks can carry a high price tag. Marinos cited a school district in Florida that was targeted by a criminal group in March. The group encrypted the district’s data and demanded a $40 million ransom to decrypt it. And back in 2019, a Kentucky school district got a fraudulent email that appeared to be from a vendor. The school ended up paying a $3.7 million invoice which went directly to an attacker.

All-in-all, 408 attacks were publicly reported in 2020, an 18 percent increase over the previous year, according to data from the Cybersecurity Resource Center that was cited in the report.

The department has taken some steps to help schools get their arms around these threats, GAO reported. The agency published guidance to help students and parents prepare for a cyberattack. It also put out guidance for schools on best practices in online learning. And it has provided schools with some resources, including training drills that have already been successful in other districts.

But “even though federal agencies do already provide a variety of products and services to help schools protect themselves against cyber threats, it’s time for them to ensure that these efforts meet current needs,” Marinos said.

Specifically, the report asks the Education Department to consult with the Department of Homeland Security’s Cybersecurity and Infrastructure Agency (CISA) to figure out how to update its plan for K-12 schools. And the GAO called for the Education Department to consider whether additional guidance is needed to protect teachers, parents, and students from cyberthreats.

The Education Department, which reviewed the report before it was published, agreed with the GAO’s recommendations, but expressed some concerns about its lack of authority over security standards for school districts.
The Dismal State of School Infrastructure, in Charts

By Mark Lieberman

A high school in Pennsylvania has leaky pipes and broken fire alarms. The ceiling collapsed at an empty elementary school in Connecticut, causing it to flood. A public pre-K facility in North Carolina found lead in its water fountains and faucets. These are just a handful of recent examples that illustrate the woefully inadequate condition of many of America’s public school buildings. Insufficient and inequitable public investment, growing nationwide K-12 enrollment, and evolving technology needs have created a situation in which thousands of school buildings are years, or even decades, behind on repairs and upgrades. Millions of students learn in buildings that are unsafe and overcrowded.

A wide body of academic research has shown that lawmakers’ inability to maintain school buildings has led to lower academic outcomes for students and a lower well-being for the teachers and administrators who spend long periods of time in school buildings.

President Joe Biden is proposing a $100 billion federal investment in K-12 school building infrastructure as part of a $2 trillion spending package that also includes funds for electrifying school buses, expanding broadband access, and eliminating the nation’s lead pipes. Congress is poised to vote on the proposal in the coming months.

Here’s how dismal the state of school infrastructure is, how we got here, and what impact Biden’s plan could have, if approved.

How big is the problem?

Millions of children travel to and from school in environmentally hazardous, diesel-fueled buses. Those kids then spend their days in buildings that are outdated, overcrowded and unsafe.

Federal, state, and local lawmakers collectively need to invest more money in order for schools to be deemed safe.

How did we get here?

School buildings have evolved to serve a growing list of functions for a ballooning number of students. But policy makers have little up-to-date data on the condition of those buildings, making it difficult for them to strategically target taxpayers’ money.

Aside from a handful of small grant programs, the federal government hasn’t invested in school infrastructure in a major way since 1935. Some states have invested far more in construction costs than others.

Overall, states invest little in school building improvements, leaving local governments to foot most of the bill. School districts in property-rich areas have a far easier time raising money to build and maintain their schools, meaning that wealthier families have more access to safer school buildings than poor families.

With minimal state and federal support, many school districts fund infrastructure projects by seeking voter approval to issue bonds and go into debt. The more debt a district has, the more interest it has to pay on that debt—money that could otherwise go toward classroom costs.

Will Biden’s infrastructure plan help?

Biden has proposed to invest more than $100 billion in America’s school infrastructure. School funding advocates say those dollars would go a long way, but they wouldn’t be enough to solve all the existing problems. That money could, however, lay the groundwork for a more concerted nationwide effort to more actively maintain school buildings for the long haul.

See charts that accompany article.

Aside from a handful of small grant programs, the federal government hasn’t invested in school infrastructure in a major way since 1935. Some states have invested far more in construction costs than others.”
Ed Tech Usage is Up. So Are Parent Privacy Concerns

By Alyson Klein

As schools ramp up their use of digital tools—and the data collection that often goes with them—parents are becoming increasingly concerned about their children’s privacy, a new survey shows.

What’s more, both parents and students want more say in how their personal information is used, according to a report released Nov. 15 by the Center for Democracy & Technology, a nonprofit organization that seeks to shape technology policy, with an emphasis on protecting consumer rights.

More than one in three parents—38 percent—listed privacy and security of their child’s data as something they are “very concerned” about, up from 30 percent one year earlier. Concern was highest among white parents, those that said they were familiar with the school’s privacy policies, and families with higher incomes.

Parents and students alike want a bigger role in deciding how schools plan to use their personal information, but often report that no one has asked for their input. Ninety-three percent of parents say it is important for schools to engage with parents or guardians about how they plan to use student data. But only 44 percent of parents report that their school district asked for their input on the subject.

A majority of parents—62 percent—also want a seat at the table when it comes to deciding what types of technology their district adopts. And 41 percent want a say when their child’s school is re-evaluating technology that’s been in use for a while.

Meanwhile, 82 percent of students said they should have a hand in figuring out how their personal data is collected and used by their school. But only a little more than a quarter—26 percent—said they had been asked for their feedback.

Students’ number one worry: a data breach that would give outsiders access to their personal records. Seventy-two percent of students surveyed said they were either “very concerned” or “somewhat concerned” about that happening.

And more than half of students—52 percent—are “very concerned” or “somewhat concerned” about their data being shared with local, state, or federal officials, including information on whether they had been vaccinated against COVID-19. Black students were especially worried about their personal records being shared with government entities, with 61 percent reporting it is something they are anxious about. High school seniors were also more likely to have concerns than younger students, with 64 percent saying this is something they are worried about.

Fifty-six percent of kids say they are “very” or at least “somewhat” concerned about “Zoombombing,” when uninvited people show up and join or interrupt class discussion. And another 54 percent say they are worried about their information—including grades, attendance, and discipline record—being shared with the local police department.

“Since the growth of online learning in response to the pandemic, our research consistently shows that edtech is here to stay,” said Alexandra Reeve Givens, the CEO of the Center for Democracy and Technology. “However, our research also shows persistent and growing student privacy concerns, underscoring the need to safeguard student privacy and support the responsible use of education data and technology.”

The survey, which was conducted last summer, included 1,001 10th grade teachers, 1,663 K-12 parents, and 420 ninth through 12th grade students.
5 Mistakes to Avoid When Spending COVID-Relief Funds

By Marguerite Roza

Imagine it’s 2023. Pundits are judging how every school district spent their Elementary and Secondary School Emergency Relief funds. There will be successes but also mistakes made in 2021 and 2022. What will those mistakes be? And what can district leaders do now to avoid them?

It’s worth recalling that the $190 billion COVID-19 relief fund is a grand experiment of sorts. The federal money is so flexible that I’m hard-pressed to find something in the rules that districts can’t use it for. While the law stipulates that 20 percent of the money be used to “address learning loss,” the remaining funds can be applied to anything deemed “reasonable and necessary.” In other words, districts have enormous latitude. That creates opportunity for game-changing spending on behalf of students—and spending blunders, too.

To wit, I share my predictions for some likely mistakes district leaders will make and some prescriptions for how to prevent them.

Mistake 1: Spending in a way that creates a disruptive fiscal cliff

Districts feel flush right now, thanks to the federal aid, but that aid disappears in 2024. And if the enrollment drops that many districts are seeing today continue, those districts will have even less money coming in from local and state sources. Districts can avoid the cliff by sticking with short-term spending commitments to match the short-term nature of the federal money versus locking in spending down the road. That means paying stipends for staff who take on extra duties and using contract staff instead of hiring new employees who expect continued employment. For districts with teacher shortages, it means using one-time hiring or retention bonuses targeting just the areas of need (say STEM or special education teachers) instead of raising base pay systemwide.

A corollary mistake is using the relief funds to offset revenue shortfalls due to permanent enrollment losses. Doing so will only delay hard decisions on downsizing the district until the aid is gone, while using up dollars in ways that may not do much to remedy the academic effects of the pandemic on students.

Mistake 2: Deploying funds inequitably across schools

State agencies now report school-by-school spending data that will make clear how much federal funding per student ultimately landed on each school. That makes it even more important for district leaders to think ahead to how spending decisions today will impact equity in the months to come. For instance, will adding one counselor to each school or an across-the-board percentage-based pay raise ultimately drive more dollars per student to wealthier schools? The answer will be yes when the wealthier schools are smaller (the counselor will cost more per student) or have more experienced teachers (because experienced teachers are paid more than less experienced ones). Similarly, districts end up using dollars inequitably when high-needs schools go months with staff vacancies or when students in high-poverty schools are less likely to participate in tutoring programs or new extracurriculars or when a facilities investment is made at just one school. One way for districts to ensure spending doesn’t flow inequitably is to deliver fixed amounts per pupil to each school (say $250 for each student plus an extra $100 per low-income or English-learner student).

Mistake 3: Issuing problematic procurement contracts that come back to haunt leaders

In many districts, 2021 will be procurement-palooza. Indeed, contracts can be great vehicles for adding capacity, for spending fast while avoiding a fiscal cliff, and for providing innovative ways to deliver services. But procurement contracts that carry even a whiff of possible problems can be trouble: Contracts tend to invite suspicion, and with new money in the mix, there are new vendors and new promises being made. Prepanademic examples of contract conflict for district leaders abound, from a no-bid contract for budgeting software in Kent, Wash., to a mammoth iPad contract in Los Angeles that led to damaging criticism of then-Superintendent John Deasy.

To prevent problems, leaders will want to follow steps that Maryland’s Montgomery County public schools took when that district agreed to pay a startup company an eye-popping $169 million annually over 16 years to lease electric school buses. Those steps include ensuring contracts have measurable outcomes with continued payment hinging on vendors hitting performance targets (and if they don’t, giving districts an out). Contracts for services with students should include measurements for student outcomes or participation rates. And contracts should be publicly vetted, voted on in board meetings, and made fully transparent (perhaps following Chicago’s lead in which every contract is online in a searchable database).

Mistake 4: Failing to make sure the school district community sees and values investments

If a tree falls in the forest and no one hears it, does it make a sound? The corollary here is: If a district makes an investment to help students and no one knows, will anyone value it? Leaving the community and school staff to wonder, “Where did all that federal money go?” is a mistake. District leaders need to reiterate what they are buying, clearly communicate the connection between investments and students, and encourage principals to engage with teachers and parents on how investments are playing out.

Ideally, district leaders keep the focus on connecting spending to goals for students. Like this: “We spent $15 million—some $125 per student—on six hours of weekly tutoring for our most vulnerable students to get them back on track in math.” That way, principals, teachers, tutors, and parents can connect the dots well after the budget is approved.

Mistake 5: Investing without demonstrating real results for students

It’s true that Congress didn’t ask for much in return for the billions in relief aid. There are no specific targets for students even though the public expects the money to help students’ learning, according to a survey of parents by the Walton Family Foundation last spring. But come 2023, if districts can’t show what they’ve
achieved for students, the spending choices are doomed to be judged a failure.

That means measuring student progress will be key. This doesn’t have to mean standardized tests (though comparing spending and outcomes by school is vital, by whatever metric is used). If spending on after-school enrichment is supposed to help lure reluctant families back to in-person school, then leaders should measure the degree to which those students are, in fact, returning. And if an investment isn’t working, it’s time to make mid-course corrections to ensure success.

With the magnitude of dollars at play, missteps are inevitable. Some district choices have already fueled alarming headlines. But plans aren’t set in stone, even after they’ve been submitted to the state. Perhaps the most important message for district leaders is this: There’s still time to modify spending decisions that won’t pass muster in the rearview mirror.

Marguerite Roza is the director of the Edunomics Lab and a research professor at Georgetown University, where she leads the McCourt School of Public Policy’s Certificate in Education Finance.
Get the information and perspective you need on the education issues you care about most with Education Week Spotlights

The Achievement Gap • Algebra • Assessment • Autism • Bullying • Charter School Leadership • Classroom Management • Common Standards • Data-Driven Decisionmaking • Differentiated Instruction • Dropout Prevention • E-Learning • ELL Assessment and Teaching • ELLs in the Classroom • Flu and Schools • Getting The Most From Your IT Budget • Gifted Education • Homework • Implementing Common Standards • Inclusion and Assistive Technology • Math Instruction • Middle and High School Literacy • Motivation • No Child Left Behind • Pay for Performance • Principals • Parental Involvement • Race to the Top • Reading Instruction • Reinventing Professional Development • Response to Intervention • School Uniforms and Dress Codes • Special Education • STEM in Schools • Teacher Evaluation • Teacher Tips for the New Year • Technology in the Classroom • Tips for New Teachers

www.edweek.org/go/spotlights

VIEW THE COMPLETE COLLECTION OF EDUCATION WEEK SPOTLIGHTS