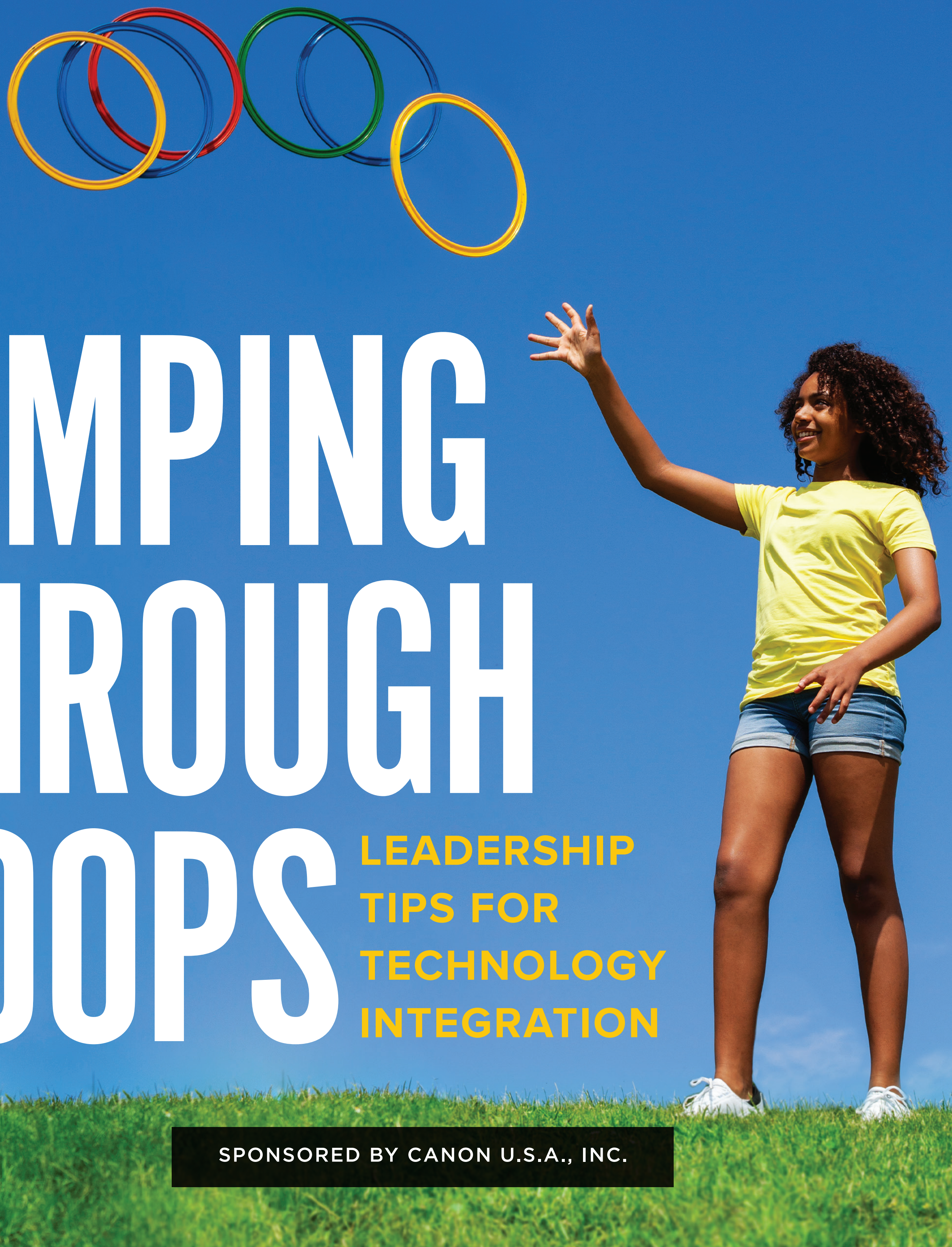
Supporting Education Business Leaders

EnvisionED K-12

VOL 6 • ISSUE 2



JUMPING THROUGH HOOPS

LEADERSHIP TIPS FOR TECHNOLOGY INTEGRATION

SPONSORED BY CANON U.S.A., INC.

CHANGE DOESN'T NEED TO BE DIFFICULT

HOW CANON CAN MAKE CHANGE SIMPLE—THE CHANGE-IT APPROACH

Nothing truly changes until behavior changes. People need to know what is coming and how it will impact them. At Canon, our approach to change is leader-led and fit-for-purpose. We work with you to scale the effort to match the scope of the change involved.

1 CLARIFY/IT

GOAL: Align leadership and make the case for change.

LEADERSHIP ALIGNMENT

Ensures that the leadership team is unified in vision and commitment.

CASE FOR CHANGE

Clearly articulates the "why" behind the change, creating urgency and setting the tone for stakeholders.

2 PLAN/IT

GOAL: Develop the roadmap and communication strategy.

ROADMAP & PLANNING

Identifies goals, milestones, and tactical steps.

COMMUNICATION PLAN

Outlines how and when stakeholders will be informed.

TRAINING STRATEGY

Prepares staff with the skills and understanding needed for success.

3 REALIZE/IT

GOAL: Execute the plan while supporting teams through change.

FAQS & SUPPORT MATERIALS

Address concerns and clarify confusion.

DASHBOARD

Provides real-time progress tracking.

LEADERSHIP TIPS & COACHING

Equips leaders to support their teams through transition.

4 SUSTAIN/IT

GOAL: Ensure long-term adoption and improvement.

FEEDBACK & ENGAGEMENT

Ongoing dialogue to address issues and gather input.

REINFORCEMENT TOOLS

Embed change into daily operations through policy, tools, and training.

PERFORMANCE MONITORING

Tracks effectiveness and identifies improvement opportunities.

WELCOME TO EnvisionED K-12
VOL 6 • ISSUE 2

CALM IN THE CURRENT

In times like these—when education finds itself caught in the crosscurrents of political scrutiny, societal pressure, and relentless change—our greatest strength as leaders may be the ability to stay cool, calm, and collected.

Technology is rewriting the playbook on how we teach and how students learn. Governing bodies are reshaping budgets in ways that make long-term planning difficult. And in some circles, people are beginning to question the very value of education itself. It's a lot.

But steady hands steer ships through storms.

"Patience, presence, and poise are the qualities that will allow us to navigate complexity without losing course."

What our communities need now are leaders who show strength not through volume, but through vision. Patience, presence, and poise are the qualities that will allow us to navigate complexity without losing course. And just as Canon's Kyosei philosophy reminds us—to live and work together for the common good—there's comfort in knowing that shared values can serve as a compass when things get cloudy.

Our cover article, "Jumping Through Hoops," explores actionable leadership strategies for navigating these hurdles, balancing the need to embrace innovative solutions with the realities of limited resources, and addressing the opportunity costs of clinging to outdated methods.

Our second feature, "Crack in the Code," delves into the growing importance of cybersecurity in K-12 education, offering actionable advice for protecting sensitive information from threats like phishing, ransomware, and unauthorized access.

This issue of *EnvisionED K-12* is packed with insight, inspiration, and practical ideas to support you as you lead. Whether you're guiding your team through tech transitions, budget constraints, or cultural shifts, we hope this content helps you lead with confidence and clarity.

Warmest wishes,
Peter Kowalczuk
EVP/Client Services Group President
Canon U.S.A., Inc.

ENVISIONED K-12 EDITORIAL BOARD

IN THIS ISSUE

Publisher
Canon U.S.A., Inc.

Managing Editor
Diana Curci

Editorial & Creative Direction
Conduit, Inc.

Get the latest insights on
envisionEDK12magazine.com

JUMPING THROUGH HOOPS

LEADERSHIP TIPS FOR TECHNOLOGY INTEGRATION

The Metropolitan School District (MSD) of Steuben County Schools' Leadership PLC meets every month to align strategies, set goals and fine tune its initiatives. The Angola, Indiana, school district also holds a Technology Leadership Cohort, which includes classroom teachers and curriculum coaches in its professional development committee. The monthly meetings help steer MSD's professional development (PD) and tech direction with real classroom insight.

In a perfect model, Chantell Manahan, Ed.D., says students would also have a voice in the meetings—a reality the administrative staff is exploring ways to make possible. In the drive for digital transformation in the K-12 environment—one where education presents a mix of exciting opportunities and persistent challenges—collective input drives collective ownership. "Educators, IT staff and administrators simply cannot operate in silos," says Dr. Manahan, CETL, MSD's Director of Technology and Chair of the Indiana CTO Council. "When you have silos, integration efforts splinter or stall."

The path to innovation is clear. The most powerful way to overcome resistance is to involve educators in the change process from the jump. When teachers feel heard, valued and supported, they are more open to taking risks. Pair that with strong modeling from leadership—leaders participating in training, co-learning with staff and being transparent about their own growth—and change becomes a shared journey rather than a top-down directive.

> **"Effective and relevant professional development is essential for helping educators learn new technologies and navigate technology transitions."**
>
> — Sharo Dickerson, MEd, Director of Digital & Learning Resources, El Paso Independent School District

Dr. Manahan believes it's essential to communicate clearly the "why" behind any change. "If educators understand how a new tool or process directly supports student outcomes or makes their work more effective, buy-in increases exponentially. Small wins, peer champions and ongoing support make all the difference. Innovation without equity is just noise. For any new initiative to scale successfully, foundational infrastructure—devices, reliable connectivity and digital literacy—must be in place for all students."

That means educational leaders must advocate relentlessly for resources, partnerships and creative solutions to close digital divides. For MSD, pilots and innovation zones are valuable testing grounds—initiatives that Dr. Manahan says should serve as stepping stones, not end points. "The goal is always to move from isolated innovation to district-wide transformation. That takes planning, listening to community needs, and designing with scalability and sustainability in mind. Tech equity isn't just a tech issue; it's a moral imperative."

With movements like Generative AI reshaping the educational landscape, professional development remains the linchpin of successful technology integration. Without it, even the best tools fall flat. To make it all come together, today's K-12 administrators must make professional development more than a one-and-done training exercise—it should be an ongoing, job-embedded strategy.

"Leadership plays a critical role in modeling learning like Generative AI," Dr. Manahan says. "When school and district leaders attend sessions, ask questions and show vulnerability in their own growth, it sends a powerful message: We're in this together. PD should also provide differentiated pathways for learners at every comfort level—offering support for early adopters and those still finding their footing. Impactful PD respects teachers' time, honors their expertise and equips them with both the skills and the confidence to lead the way."

LEARNING TO JUGGLE

Located in El Paso, Texas, the El Paso Independent School District (EPISD) is the largest district in the Texas Education Agency's Educational Service Center – Region 19. With nearly 50,000 students in 75 campuses, EPISD, which was organized in 1883, employs nearly 9,000 people.

From where Sharo Dickerson sits, districts like EPISD face several significant challenges that hinder their ability to integrate technology into the learning environment effectively. One of those is limited funding and resources, which often result in inadequate financial support for purchasing and updating devices, upgrading infrastructure and providing ongoing technical maintenance.

> "The goal is always to move from isolated innovation to district-wide transformation. That takes planning, listening to community needs, and designing with scalability and sustainability in mind."
>
> — Dr. Chantell Manahan, CETL,
> Director of Technology,
> Metropolitan School District of Steuben County

Additionally, there often is a lack of sufficient training and professional development opportunities for end-users and stakeholders, making implementing current and innovative technologies relevant to teaching and learning difficult. “Outdated technical infrastructure further complicates matters,” says Dickerson, MEd, EPISD’s Director of Digital and Learning Resources. “It impacts bandwidth performance and connectivity, affecting consistent and meaningful implementation of technology initiatives.”

Facing these types of issues day in and day out can lead to a hesitation and resistance to change within the school environment—pushback that leads to limited progress in adopting new methods that could enhance student and teacher success. “School leaders can promote collaboration among educators, IT staff and administrators to develop a cohesive technology integration plan by establishing a shared vision that resonates with and involves all stakeholders,” Dickerson says. “It is crucial to create structured communication channels among the Academics, Information Technology and School Leadership divisions to ensure everyone understands the institutional goals behind the technology plan.”

Dickerson also believes that stakeholders can enhance effective collaboration by employing design thinking approaches to address diverse perspectives, implementing decision-making frameworks to clarify roles and responsibilities and offering professional development opportunities to understand the classroom’s needs better.

“Effective and relevant professional development is essential for helping educators learn new technologies and navigate technology transitions,” Dickerson says. “What does this look like? Professional development becomes a positive experience when educators receive technical skills and a pedagogical understanding of integrating technology. This includes providing differentiated learning pathways based on the educators’ experience levels, offering follow-up support for technology integration during Professional Learning Communities (PLCs), delivering training through online platforms, and ensuring that technology integration training is directly connected to curriculum and instructional priorities.”

In today’s K-12 landscape, digital transformation is more than adopting new tools; it’s about creating equitable, forward-thinking systems that serve all learners. By leading with intention, schools can turn today’s challenges into tomorrow’s opportunities for lasting impact.

CRACK IN THE CODE

BEST PRACTICES FOR CYBERSECURITY IN K-12 EDUCATION

Each week, the staff at Community High School District 99 receive a brief scenario-based form prompting them to think critically about how they would respond to various cyber and physical security situations. The initiative—which the Downers Grove, Illinois, district branded "What-If Wednesday"—encourages ongoing reflection and engagement with its security protocols.

Tony Dotts, District 99's Information Security Manager, says that staff training plays a vital role in defending against cyber threats, as even the most advanced security tools cannot fully compensate for the human element. As schools rely more on digital platforms, safeguarding student and staff data continues to be a critical priority. Part of that safeguard means empowering staff with knowledge and awareness.

"It's important that staff not only understand what data we're protecting, but also understand their role in maintaining its security," says Dotts, CISSP, CvCISO, CETL, CCRE. "Our initial training effort was through simulated phishing campaigns. These exercises help staff identify the signs of phishing attempts and understand the correct procedures for reporting them."

By clearly communicating the purpose of these simulations and offering immediate, constructive feedback—including targeted mini-trainings for those who fall for phishing attempts—the District 99 team fosters a culture of learning rather than punishment. "Over time, we've expanded our training approach to include a variety of methods to reach different learning styles and maintain ongoing engagement," Dotts says.

Some of those approaches include things like professional development sessions, where the full administrative team partakes in a four-hour tabletop cybersecurity exercise simulating realistic scenarios and discussing appropriate responses. Another checkpoint is new staff onboarding, in which all new hires are required to complete a concise, 15-minute cyber safety training video to establish a baseline understanding from Day 1.

Other tools include visual reminders, including cybersecurity posters and digital signage placed in high-traffic areas to provide ongoing, passive reinforcement of key safety messages, and periodic email reminders tied to relevant threats, such as seasonal scams or phishing trends observed in the wild.

"We face the same types of attacks as Fortune 500 companies but without a Fortune 500 budget," Dotts says. "The most common threats are ransomware, phishing, and social engineering, which are often interconnected parts of the same attack. Our data—especially student Personally Identifiable Information (PII)—is valuable, and schools are particularly vulnerable because we're seen as soft targets."

Many school districts today lack the resources for dedicated cybersecurity staff and tools, giving attackers an advantage. Additionally, the complexity of school IT environments, spanning both on-premises systems and the cloud, further increases the attack surface.

AT THE READY...

William Brackett recalls an incident at another school district where a cyber attacker used credentials from a website breach to gain initial access to the district's system. In the following months, a team of attackers was able to move laterally until they found administrative credentials. Once they had administrative access, they planned a ransomware attack.

During an evening on a weekend right before a district break, the attackers set out to launch their attack. Before doing so, they threatened to release PII data from the school district, which resulted in a ransom being paid. The IT team were alerted within 12 hours of the start of the attack. After third-party entities were brought in, the IT team successfully cleaned up the backups and rebuilt the network. By the time the students came back from break, the district was at 90% operational capacity.

While Oak Park Elementary District 97 has never had a major breach of its systems, Brackett, Director of IT Services for Oak Park, is a student of what has happened at other districts and how they handle breaches. "Cybersecurity attacks follow what some call the anatomy of an attack, which I refer to as a chain of attack. In these models, it starts with initial access. The chain follows a series of attacks laterally and vertically to find the useful or intended resources to exploit."

Brackett says for too long, security and data privacy have been a secondary or afterthought for many school districts. Efforts become bolt-on pieces that have inherent weaknesses. "We need to start working on designs and systems with security as part of the design. We also need to demand that our vendors' offerings are secure by design as well."

> "We need to start working on designs and systems with security as part of the design. We also need to demand that our vendors' offerings are secure by design as well."
>
> — William Brackett, Director of IT Services,
> Oak Park Elementary District 97

There are many different methods of training for today's school administrators. One of the ways is to interject cybersecurity training into compliance training, which while an easy way to get eyes on the content, is the least effective. Another is phishing testing, along with training, which gives data on the readiness of staff while providing feedback training for those who failed the test.

The most effective method is the one that takes the longest—teachable moments. "This takes the form of a one-on-one review of an incident," Brackett says, like the one that hit Oak Park. "It requires using After Action

Reviews (AAR) to build an environment of learning from actions. We also use group reports on known incidents and mass email attacks. I would explain the attack and how it was detected, praising staff members who identified the issues publicly."

Oak Park's IT team builds systems and trains staff on the processes, stressing that they will never get reprimanded for holding to the process. "The more sensitive the department, the stronger the processes and reinforcement," Brackett says.

BUILDING YOUR CYBERSECURITY PLAN

One of the most comprehensive cybersecurity plans for K–12 education begins with a foundational assessment, ideally based on the NIST Cybersecurity Framework. While the full framework can be overwhelming, there are free, K–12-specific assessment tools that help schools understand and apply its principles in a manageable way. These assessments are invaluable for identifying strengths, pinpointing areas for improvement, and outlining the steps needed to enhance cybersecurity posture.

Both Dotts and Brackett favor this approach. In addition, key components of a strong plan include an Incident Response Plan and a Business Continuity Plan—often referred to in educational settings as a Learning Continuity Plan. Both are essential for ensuring that teaching and learning can continue with minimal disruption during a cyber event.

Policy development is another critical area. In District 99, Dotts and his team partner with their Incident Response vendor to update and refine a range of cybersecurity policies—from Acceptable Use and Asset Management to Security Training, Vulnerability Management, and more. These are all consolidated in their public-facing Information Security & Data Privacy Governance Guide, which serves as a central resource for staff and stakeholders.

For schools with limited budgets, starting with a focused assessment and building out practical, scalable policies and response plans offers a strategic path forward. "It is a sad truth that funds for cybersecurity are a low priority," Brackett says. "Board members and administration see 'what if' spending versus spending to address student achievement. When that formula is considered, student achievement will always win over cybersecurity spending."

STRENGTHENING YOUR CYBERSECURITY STRATEGY

A comprehensive cybersecurity strategy doesn't require a massive budget—it requires a smart, balanced approach. Start with a foundational self-assessment using the NIST Cybersecurity Framework or CIS Critical Security Controls, which help identify current strengths and gaps. From there, build out key components:

INCIDENT RESPONSE & LEARNING CONTINUITY PLANS

Minimize disruption during a breach.

POLICY DEVELOPMENT

Cover areas like Acceptable Use, Asset Management, Security Training, and more.

CYBERSECURITY CULTURE

Train staff regularly, and set secure-by-default expectations within your tech team.

ENDPOINT PROTECTION

Use built-in tools to encrypt data, restrict admin access, and configure local firewalls.

NETWORK MONITORING

Set up logging and learn what "normal" traffic looks like to spot anomalies early.

Source: Tony Dotts, Information Security Manager, Community High School District 99; William Brackett, Director of IT Services, Oak Park Elementary District 97

In today's digital learning environments, safeguarding student data and school infrastructure requires more than just firewalls—it demands a culture of cybersecurity awareness and proactive planning. By implementing best practices and fostering collaboration across IT teams, educators, and administrators, K–12 schools can stay one step ahead of evolving threats. ■

TECHNOLOGY & AI IN EDUCATION

AI INTEGRATION

75% of K–12 students reported using AI tools in 2024, a significant increase from 37% in 2023.[1]

51% of K–12 teachers utilized AI tools for tasks such as lesson planning and assessments.[1]

EDTECH ENGAGEMENT

Over 57 billion interactions were recorded across more than 9,000 educational technology products during the 2023–2024 academic year.[2]

57 BILLION INTERACTIONS

Source: 1 - https://tinyurl.com/2024-AI-Education, 2 - https://tinyurl.com/EDTechRise

ACADEMIC PERFORMANCE & LEARNING LOSS

-2 pts

Reading Proficiency

Average reading scores for both fourth and eighth graders in 2024 dropped by two points compared to 2022 and five points since 2019.

1/3 One-third of eighth-grade students scored below the “basic” level in reading, marking the lowest performance in over three decades.

Source: https://tinyurl.com/USStudentReading

+2 pts

Mathematics Achievement

Fourth-grade math scores saw a modest increase of two points since 2022 but remain three points below pre-pandemic levels.

Eighth-grade math scores remained unchanged from 2022 and have not returned to 2019 levels.

Source: https://tinyurl.com/USMathStats

FUNDING & SPENDING

Per-Pupil Expenditure

The average spending per student in public K–12 schools was $17,277.[1]

Total Public Education Expenditure

Nationwide, public K–12 education expenditures totaled $857.2 billion, accounting for 3.67% of taxpayer income.[1]

Federal COVID-19 Relief

Since fiscal year 2020, the U.S. Department of Education has allocated $186 billion in COVID-19 relief funds to support pre-K through secondary education.[2]

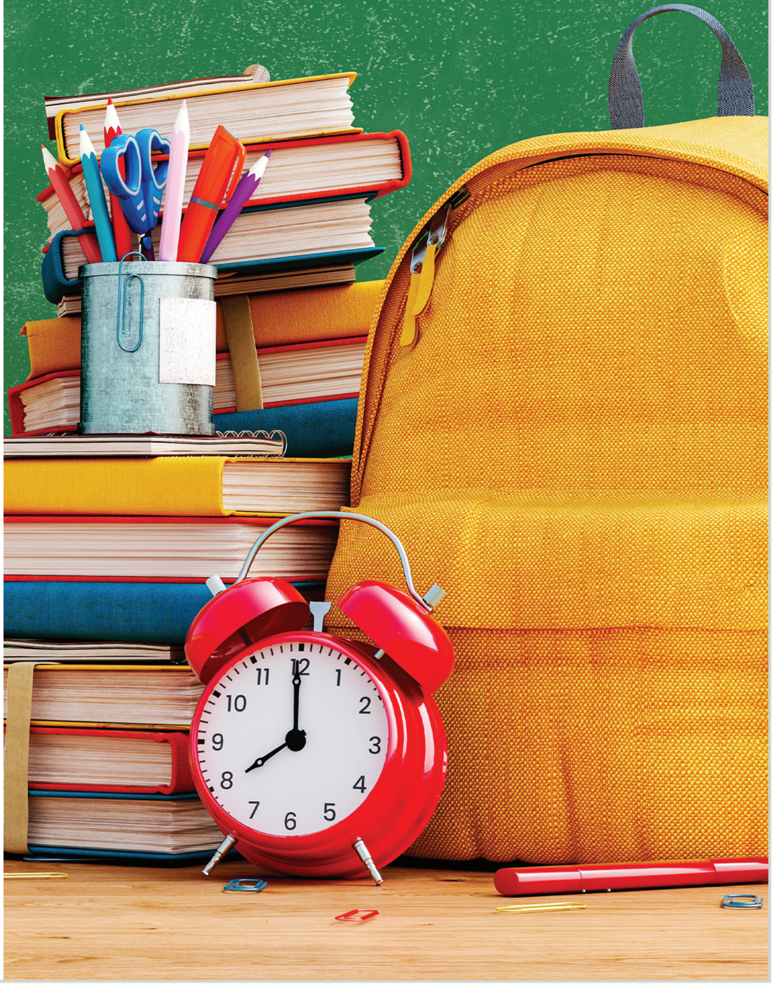
Source: 1 - https://tinyurl.com/USPublicFunding, 2 - https://tinyurl.com/USDeptData

FUTURE ENROLLMENT PROJECTIONS

-2.7 MILLION PUBLIC SCHOOL STUDENTS

Declining Enrollment Forecast

Projections indicate a decrease of 2.7 million public school students between 2022 and 2031, reducing total enrollment to approximately 46.9 million.



Q&A

Talking with...Kelly May-Vollmar & Ruben Garza

Ed.D., Superintendent of Educational and Technology Services, Desert Sands Unified School District
Manager of Computer Network Services, Desert Sands Unified School District

Securing the Digital Campus

A Q&A on Cybersecurity in K-12 Education

In today's digitally driven K-12 landscape, cybersecurity is no longer optional—it's essential. As schools integrate more technology into their teaching and operations, the risks grow alongside the rewards. To explore the evolving challenges and solutions, we sat down with two forward-thinking leaders from Desert Sands Unified School District (DSUSD) in California.

Dr. Kelly May-Vollmar is Superintendent of Educational and Technology Services for DSUSD, where she serves 27,000 students. A recognized voice in digital equity and educational leadership, she is a CoSN Board Member and the recipient of several national and state honors, including the 2024 DALI Women of Distinction Award. Her leadership helped DSUSD launch its own LTE Network and win the CoSN Digital Equity Award.

Ruben Garza, Manager of Computer Network Services at DSUSD, has over two decades of experience in IT across K-12 education, law enforcement, and healthcare. He brings a security-first mindset to school operations, leading initiatives that safeguard infrastructure while enabling student success and instructional continuity.

What are the most common cybersecurity threats facing K-12 schools today, and why are schools particularly vulnerable to these attacks?

Ruben Garza: Malware attacks targeting students are increasingly common and occur daily. K-12 schools are especially vulnerable because students often engage in risky online behavior—like downloading free software or games—without understanding the risks. Combine that curiosity with limited cybersecurity awareness and under-resourced IT teams, and you've got an easy target for malicious actors.

Dr. Kelly May-Vollmar: Adding to that, limited budgets often prevent districts from investing in robust cybersecurity tools. Outdated systems and the inability to offer competitive salaries make it hard to attract top cybersecurity talent, leaving schools exposed.

Can you share a specific example of a security breach in a school district and the steps taken to recover and prevent future incidents?

Garza: In one incident, students received phishing emails disguised as job opportunities. These emails asked for personal phone numbers and, later, small payments to "complete" job applications. In response, we implemented targeted email filtering policies that block messages containing suspicious phrases like "Part-Time Work At Home" or "Job Opportunity For All Students." These proactive filters have significantly reduced phishing attempts reaching students.

How can leaders balance the need for robust cybersecurity measures with maintaining a user-friendly experience for students and staff?

Garza: Cybersecurity should work in the background. The right tools enhance protection without disrupting productivity or learning. If users feel friction, it's probably the wrong solution. Seamless integration is the goal—security that feels invisible but effective.

> "Cybersecurity should work in the background. The right tools enhance protection without disrupting productivity or learning."
>
> — Ruben Garza, Manager of Computer Network Services, Desert Sands Unified School District

What role does staff training play in protecting against cyber threats, and what are effective ways to implement such training in a school setting?

Garza: Cybersecurity awareness is your first line of defense. Students and staff are prime targets for phishing and social engineering. Ongoing, engaging, and relevant training—including phishing simulations and bite-sized learning modules—goes a long way.

May-Vollmar: We've mandated annual cybersecurity training for all staff and supplement that with ongoing sessions highlighting current threats. Our users are often the weakest link, so training them to be our strongest defense is a priority.

What are the key elements of a comprehensive cybersecurity plan for K-12 education, and how can schools with limited budgets prioritize their efforts?

Garza: A strong plan includes access controls, endpoint protection, regular backups, staff training, and an incident response protocol. Start with foundational protections—multi-factor authentication, good password hygiene, and user education. Also, explore free resources from government and nonprofits to stretch your dollars.

May-Vollmar: Leadership buy-in is also critical. Security must be a visible priority across the organization. Create a culture of open communication so staff feel safe reporting concerns, and adopt a continuous improvement mindset—review, revise, repeat.

> "Our users are often the weakest link, so training them to be our strongest defense is a priority."
>
> — Dr. Kelly May-Vollmar,
> Superintendent of Educational
> and Technology Services,
> Desert Sands Unified School District

How do you see the role of cybersecurity evolving in K-12 education as schools adopt more advanced technologies?

Garza: Cybersecurity is becoming increasingly reliant on automation and AI. The threats are more complex and frequent, while staffing remains limited. AI-driven tools will be essential to monitor, detect, and respond to attacks in real-time across expanding digital environments. 🟥