WORKING TOGETHER FOR STUDENT SUCCESS

A GUIDE FOR SBOS & CTOS

ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

CoSN
Leading Education Innovation

CONTENTS

ABOUT THIS TOOLKIT

This toolkit was created by the Association of School Business Officials International (ASBO) and The Consortium for School Networking (CoSN) to help ASBO and CoSN members understand the value of a school district's business and technology departments working together. This toolkit is the 2nd edition (updated in 2024).

This resource identifies some common issues impacting the roles of school business officials (SBOs) and chief technology officers (CTOs) and shares best practices, tips, and tools to address them. We hope this toolkit is useful in highlighting areas of opportunity for business and IT office collaboration to help support your school district's education goals and increase students' chances for success.

A special thanks to all ASBO International and CoSN members who contributed to this technology toolkit. Without the help of these volunteers, this project would not have been possible. Readers may find a full list of individuals who helped create this resource in the Appendix.

Questions? Contact ASBO International at 866.682.2729 or asboreq@asbointl.org and CoSN at 202.558.0059 or membership@cosn.org.

ABOUT ASBO INTERNATIONAL

The Association of School Business Officials International (ASBO) provides programs, resources, services, and a global network to school business professionals who are passionate about quality education. ASBO International promotes the highest standards of school business management, professional growth, and the effective use of educational resources. ASBO members are the finance decision-makers in school systems around the world who manage budgeting, purchasing, facility operations and maintenance, human resources, technology, transportation, food service, healthcare, and many other areas that affect the business and operations aspects of education. Learn more at asbointl.org.

ABOUT CoSN

CoSN, the world-class professional association for K–12 EdTech leaders, stands at the forefront of education innovation. We are driven by a mission to equip current and aspiring K–12 education technology leaders, their teams, and school districts with the community, knowledge, and professional development they need to cultivate engaging learning environments. Our vision is rooted in a future where every learner reaches their unique potential, guided by our community. CoSN represents over 14 million students and continues to grow as a powerful and influential voice in K–12 education.

WORKING TOGETHER: SBOS & CTOS ARE VALUABLE PARTNERS

School business officials (SBOs) and chief technology officers (CTOs) have varied responsibilities when it comes to school district operations. However, their duties often cross paths. So why do alone what you can do better together?

Breaking down the silos between the business and IT offices and building a solid working relationship benefits the school district in many ways, including increased staff productivity and efficiency, and positive spillover benefits for overall district operations, educational services, and student achievement. Failing to work together is a missed opportunity to free up more time and resources to focus on what matters: student success.

For SBOs and CTOs to work together effectively, they must first understand each other's roles. By understanding where duties overlap, the business and technology teams can identify new areas for collaboration. Below are two frameworks that outline the essential skills, knowledge, and tasks for what successful school business and technology leaders look like.

ASBO International's International School Business Management Professional Standards	CoSN's Framework of Essential Skills of the K–12 CTO
The Educational Enterprise	Leadership & Vision
Financial Resource Management	Strategic Planning
Human Resource Management	Ethics & Policies
Facility Management	Instructional Focus & Professional Development
Property Acquisition & Management	Team Building & Staffing
Information Management	Information Technology Management
Ancillary Services	Communication Systems Management
	Business Management
	Data Management
	Data Privacy & Security

After reviewing the frameworks above, schedule a meeting with your SBO or CTO partner to discuss your roles, assess how each of you measures up with your respective professional standards, and identify areas where your offices should collaborate based on where your responsibilities overlap.

Here are some questions to help you reflect as you review:

- How do my skills as an SBO or CTO align with the standards of my profession? Where am I meeting these standards and where is there room for improvement?
- How aware am I of my colleagues' responsibilities in the business/IT department? Am I familiar with the delegation of duties?
- How is the IT/business office currently working together? Are we only working together on IT/financial issues?
- Are there other areas of district operations where we could be collaborating more—for example with district leadership and strategic planning, instructional support, or ancillary services?

Sources/More Reading:

ASBO International: International School Business Management Professional Standards

CoSN: Framework of Essential Skills of the K–12 CTO

NEED HELP GETTING STARTED?

Think of all the ways SBOs interact with technology in their district every day to identify potential collaborative opportunities.

Managing Resources Responsibly
SBOs work extensively with financial, human resources (HR), and administrative data. What would they do if they had to manage that data manually, without technology's help? How difficult would it be to report where district funds are coming/going? Could they easily show how dollars are linked to student learning? CTOs can help SBOs ensure they have the right IT software and solutions to identify relevant data for making informed financial decisions.

Engaging Education Stakeholders
School districts are responsible for engaging with students and parents about the educational programs they offer. Without a functioning website, secure email system, or responsible social media presence, how well can the district share information with the public? If there is an emergency, how can staff understand and relay what happened and effectively respond? Technology speeds up communication and plays a major role in risk management, so SBOs and CTOs should cooperate to protect students and staff and maintain a positive district image.

Maintaining Business Continuity
What do you do when you log onto your computer and a message appears that reads, "The network is currently not available"? When all systems are down—business, student information, classrooms, food service, security/alarms, building automation, phones—who do you call for help? All school systems are powered by technology, which also enables education delivery, so SBOs need to work closely with their IT team on a business continuity program to keep business running as usual.

Other Ideas for Collaboration

1. **Launching a new technology initiative** (AI courses and training, environmental sustainability, e-learning, remote learning, VR/AR technology, new STEM courses, creating makerspaces, etc.).

2. **Improving school security** (cybersecurity and student data privacy governance, improving privacy and security to better protect student and employee personal data and school financial information, including creating and maintaining secure system and data backups, conducting privacy, security, and IT assessments/audits, adding filters/censoring websites per applicable CIPA requirements, thoughtful, limited monitoring student web activity, and measures such as cameras and door security to protect the physical environment, etc.)

3. **Leveraging IT to achieve efficiencies** (implementing software to streamline operations, building a new information database, improving interoperability, going paperless, standardizing workflow processes, improving transportation and energy systems, etc.).

4. **Investing in infrastructure** (purchasing hardware and software, improving network capacity for online learning, disaster preparedness, passing bonds to upgrade IT or other infrastructure, etc.).

Sources/More Reading:

Critical Skills for Today's CTO
7 Areas to Collaborate with Your IT Office
Finding Gold in Data Mining
Environmental Sustainability for Technology
Blaschke Report: Navigating Student Device 1:1 Sustainability
School Safe Technologies
Disaster Preparedness
Cybersecurity Governance
Student Data Privacy Governance
Trusted Learning Environment Seal
Interoperability

FIRST STEPS FOR BUILDING A POSITIVE RELATIONSHIP

Maybe you don't have the closest relationship with your SBO or CTO yet and need a little nudge. Consider these tips to help you build a positive relationship.

1. **Meet early on (preferably one-on-one) to get to know each other. Invite your colleague to grab coffee or lunch.**
   - Relationships are founded upon recurring, face-to-face meetings over time. Frequent interactions help build familiarity and trust.
   - Discuss each other's processes, procedures, expectations, goals, challenges, etc., to help understand each other's scope of responsibilities. Colleagues must clearly communicate who they are and what they do to work together effectively.
2. **Schedule an introductory staff meeting to help your business and IT teams get to know each other, too. Plan a team building activity to help break the ice.**
   - Schedule ongoing cross-departmental meetings to build team trust and morale. These meetings can allow staff a chance to share their areas of focus and project status updates.
   - Breaking down silos and improving teamwork between the business/IT offices is beneficial to problem-solving and innovation. Putting several heads together can help identify an out-of-the-box solution or potential issue before a problem arises.
3. **Remember that your and your colleagues' areas of expertise are not the same.**
   - Be patient and understanding when communicating and sharing perspectives. Finance and IT specialists speak their own language, and that "curse of knowledge" can prevent you from clearly communicating with and understanding your peers.
   - Although your expertise may differ from your SBO or CTO, everything you and they do affects every aspect of the district, from resource management and strategic planning to classroom instruction and student services. Each person's contributions are valuable and critical to the district's overall success.

Sources/More Reading:

The Innovation Code: The Creative Power of Constructive Conflict

EDUCATION RESOURCE MANAGEMENT

Challenge/Opportunity: With scarce funding and growing demands for accountability, SBOs and CTOs must collaborate to ensure IT and educational investments deliver value and high returns for student learning, well-being, and success.

EVALUATING THE MERIT OF NEW TECHNOLOGY INITIATIVES

SBOs and CTOs can work together to determine if a new technology initiative is worth the district's time and resources. They can evaluate the reasonableness of a request by determining whether the initiative makes sense, is systemic, and is sustainable.

When presented with a request for a new initiative, consider:

- Does the proposal make sense for the entire organization? Can it be implemented throughout the district?
- Is it possible to sustain the initiative over time? Will it receive "one-time" funding that may not be available in the future?
- How will the program's hardware and software be replaced or upgraded 3–5 years from now? Has adequate funding been allocated for teacher and/or staff professional development?

If the answer is "yes" to these questions, the proposal should be further considered for piloting or full implementation. If not, SBOs and CTOs should give pause before approving the request.

Sources/More Reading:

How to Evaluate Requests for New Technology Initiatives

Network and Systems Design Resources

IDENTIFYING AREAS TO FIND EFFICIENCIES

Since budgets are always tight, SBOs and CTOs can help each other identify the wisest areas to invest in and cut programs with minimal impact on district operations. They can seek input from other departments to identify how technology is being used, where staff can manage cutbacks in hardware, applications, and support, and how IT could be further leveraged to support staff productivity and student learning. SBOs and CTOs also can calculate returns on investment (ROI) and the value of investment (VOI) to weigh the pros and cons of IT investments and share that data with stakeholders to justify specific decisions.

TIP: Consider these ideas for improving IT efficiencies and reducing costs in your district.

- Standardize on cloud-based email.
- Replace old computers and reduce the number of operating systems supported.
- Use IT asset management to track computers and application usage.
- Use self-services for data entry and go paperless where possible.
- Implement centralized user support tools and computer software upgrades.
- Evaluate the purchase of spare equipment versus extended warranties.
- Leverage volume purchasing with vendors through multidistrict contracts.
- Restructure service contracts and negotiate lower vendor maintenance charges.
- Lease or purchase refurbished equipment to replace old technology.
- Discard personal printers and consolidate print-copy center devices to multifunction.

Sources/More Reading:

Getting the Most from IT

Budgeting, Total Cost of Ownership (TCO) & Value of Investment (VOI)

INVESTING WISELY TO BOOST DISTRICT GROWTH

Technology investments can make a major difference in a district's growth, decline, or stagnation. Whether you need to replace outdated IT systems or determine the most appropriate school success solutions, SBOs and CTOs should consider these strategies.

1. **Look for IT systems that link expenditures to achievement.** Find a comprehensive administrative/management software system that includes tools that tie spending to growth (e.g., streamlined grade book processes, efficient human resources functions, curriculum tracking, and parent access portals). This will save the district time and money.

2. **Remember that all district data must be managed in ways that can help administrators, teachers, and other stakeholders make sense of it.** Powerful reporting and analytics programs can integrate data gathering and analysis from all operational and educational aspects of district administration, while simultaneously revealing ROI and VOI.

3. **Ensure the IT system includes training and support as needed.** Every stakeholder must be able to understand and take advantage of the full benefits of their programs. A robust IT system provides information about data collection and analysis; IT personnel offer users opportunities to learn what the data/systems mean for continuous improvement.

4. **Understand that strategic planning must drive IT spending.** All IT expenditures should support the school board's and community's envisioned future and the district's mission. This alignment is critical.

Sources/More Reading:

Five Ways IT Spending Boosts District Growth

Driving K–12 Innovation Report

Guide to Leverage CoSN's Driving K–12 Innovation Report

CONDUCTING TECHNOLOGY AUDITS OR PEER REVIEWS

Schools are ramping up technology use as a teaching tool and administrative asset for staff and students, but increased adoption means more work for SBOs and CTOs who must manage, secure, and optimize multiple devices across the district's network infrastructure.

A technology audit or peer review can help districts assess the effectiveness of technology for administrative and instructional purposes and identify the status and location of all district IT assets. Audits play an important role in meeting IT readiness requirements, managing software licenses and inventory, capital planning, and more. Knowing which assets you have, how they're used, and who's using them is critical to efficient, cost-effective resource management.

4 Steps for Effective IT Audits

1. **Determine whether the audit or peer review will be conducted internally or externally.**
   - Audits can be conducted by district staff or a third party. Regular audits can improve compliance, protect assets, minimize unauthorized installations, and provide a plan for future upgrades/replacements—but be aware that they also can place a burden on staff in terms of time and resources.

2. **Gather vital information via document reviews, surveys, and interviews to obtain an accurate picture of K–12 technology use.**
   - Review the district's strategic plan, technology plan, budget, organization chart, professional learning plan, and special program plans to provide perspective on how important the technology is and how it is being implemented.

- Identify all IT assets, such as PCs, tablets, and notebooks; component parts and servers; printers; networking/telecommunications equipment; projectors; security systems; and software. IT audit software and automation can assist with this task.
- Gather insights about the effectiveness of the technology program by surveying parents, students, teachers, and administrators to get a more detailed picture of technology use as well as challenges.
- Use survey results to create more insightful questions and incorporate them in formal interviews with key stakeholders. Use their responses to clarify specific issues and further refine data already gathered.

3. Create the audit or peer review report.

- Include the current state of technology use. Start with evidence of the success of technology-driven programs in the district, then provide an analysis of the data gathered and a list of recommendations.
- Districts often don't have the in-house expertise needed to analyze data and establish a baseline to determine the implementation level of all its various technologies. If hiring a consultant, find someone who knows education technology and has a broad understanding of the district's instructional needs.
- The report's recommendation section should state the current condition, suggest ways to improve it, and examine other impacted items to determine what changes are truly needed. For instance, a technology integration peer review may find that technology infrastructure must also be addressed to encourage technology use (if currently inadequate) and may recommend teachers receive professional training to increase the chances for adoption and integration, too.

4. Provide a roadmap for district improvement.

- A helpful audit or peer review report provides the district with a general road map for improvement; the most helpful road map is a model that includes a rubric.
- An audit report or peer review is just a report. Improvement depends on whether the district incorporates the findings of the report into its plans and practices.

Sources/More Reading:

Peer Review vs. Technology Audit

CoSN Peer Review Resources

Conduct Your Own Technology Audit Using CoSN's Framework

LEVERAGING IT TO IMPROVE STUDENT EQUITY

Students with limited or no high-quality Internet access at home are at a disadvantage when compared to their well-connected peers. SBOs and CTOs must work with other K–12 leaders to reduce the access gap for learning and can consider these strategies to address digital access.

How Can SBOs and CTOs Address the "Digital Access" or "Homework" Gap?

1. **Utilize publicly available data to understand the scope of the problem.** CoSN's Digital Access Resources have innovative and practical tools designed to help school districts and communities leverage data to close digital access gaps.

2. **Survey the community to gain additional insight into the scope of the problems.** Teachers and administrators may be able to identify specific students without home Internet access; however, school districts should quantify the issue via available data. Consider bundling home access surveys with other forms distributed at the start of the school year and/or to new students.

3. **Identify community areas for access.** Explore partnerships with libraries, community organizations, and businesses to provide Wi-Fi hotspots for students without home Internet access. Research online for information about local organizations to partner with.

4. **Promote low-cost broadband offerings.** Many Internet Service Providers (ISPs) offer discounted Internet plans for low-income households. However, some companies only provide discounts for a limited time and restrictions can exist, so read the fine print first.

5. **Deploy mobile hotspot programs.** These programs can be an effective digital access strategy, especially for students living in households that frequently move and for whom low-cost wired broadband plans may not be an effective solution. Note that some hotspots cap bandwidth monthly, and several factors affect how much data students will need (e.g., basic web research, email, and learning management systems don't require as much data as streaming videos or downloading large files).

6. **Install Wi-Fi on school buses.** More districts are installing Wi-Fi on school buses to allow students to do daily homework during their commute or when traveling to after-school activities. Federal E-Rate funding now supports Wi-Fi on buses. Also, bus Wi-Fi connectivity can reduce behavioral problems while in transit.

Improving Digital Equity Requires a Holistic Approach

Solving the "access gap" isn't the only challenge for improving digital equity. Whether education leaders are looking to bring broadband to a rural area, or simply take a broader approach to digital access and inclusion, community collaboration is a powerful tool. After all, access isn't just a school or district problem—it's a community problem. Regardless of the initiative, here are some steps to help you work toward your digital access goals.

1. **Assemble a coalition and develop a shared vision.** Engage local elected officials, community organizations, libraries and other educational institutions, social service facilities, local governments, chambers of commerce, and others.

2. **Assess existing community resources, gaps, and needs.** Identify existing physical and human capacity community resources, conduct a needs assessment, and determine what structures/systems are needed to implement and sustain digital access efforts.

3. **Engage stakeholders and partners.** Seek community input about the best way to move forward. Strengthen relationships, seek areas of agreement, and bring a wider range of constituents together to form a common vision for the future.

4. **Develop and execute a project plan.** Include input from all stakeholders, create detailed project timelines and deliverables, and use contracts/other documentation to ensure all parties understand their roles and responsibilities. Appoint a project manager and planning team to meet regularly to evaluate progress and refine processes as needed.

Sources/More Reading:

CoSN's Digital Access Resources

What You Need to Know About the Homework Gap

FCC Announces E-Rate Funding Can Support Wi-Fi on School Buses

IDENTIFYING REVENUES TO FINANCE TECHNOLOGY INITIATIVES

SBOs and CTOs can help each other identify funding sources for IT projects at the local, state, and federal levels. Here are some strategies and options to consider for financing specific endeavors.

1. **Prioritize your needs before pursuing funding options.** Implement a strategic planning process to evaluate the required resources, responsibilities for implementation, and adherence to current legal and policy guidelines. Use that strategic plan to prioritize needs, avoid arbitrary decisions, and ensure resources align with district goals.

2. **Join discount programs for competitive pricing.** Engage with state or local government discount initiatives similar to regional consortiums, which offer competitive pricing for IT hardware, software, and services through efficiently negotiated contracts.

3. **Leverage no-interest financing options.** Utilize financing options from vendors that provide installment payments without interest, aiding in easier budget management and financial planning.

4. **Research various grants to meet your needs.** Explore grants designed to enhance the use of technology in education, such as those supporting telemedicine and distance learning, especially in rural areas. Also, consider applying for cybersecurity funding from national programs that help protect educational institutions from cyber threats and enhance their digital infrastructure.

5. **Use all the tools in your toolbox.** Explore diverse financial resources, including annual budgets, bonds, specialized state funding, federal programs, and other relevant grants to support technology advancements and infrastructure development.

K–12 Tools to Finance Your Technology Goals

User Fees

Collecting reasonable fees for student technology use may be an option depending on local district and state policies. Some schools charge general usage or insurance fees to cover ongoing costs of repairing and replacing hardware and to mitigate damage and loss.

Bonds and Levies

Local voter-approved funding proposals can be leveraged to finance large technology upgrades and improvements. However, early planning and consistent follow-through are critical to help ensure successful bond or levy passage. When SBOs and CTOs work together on a bond campaign, they can increase the district's chances for success for voter approval. They can help each other create a realistic timeline and vision statement to ensure it reflects the district's mission, obtain buy-in from other district leadership, determine the best launch time to increase turnout and support, and collect data to communicate the project's benefit to the public.

E-Rate Discounts and Reimbursements

Also known as the Universal Service Program for Schools and Libraries, this federal program is run by the Federal Communications Commission (FCC) and funded via the Universal Service Fund (USF). E-Rate offers discounts and reimbursements for telecommunications, Internet access, and internal connections for eligible schools and libraries. Discounts range from 20–90% based on school poverty level, and higher discounts are available for rural schools and libraries.

Every Student Succeeds Act (ESSA) Title IV-A Grant

ESSA's Title IV-A program is a federal block grant that can fund district projects to 1) provide students with a well-rounded education, 2) support safe and healthy students, and 3) support the effective use of technology. Note that funding is subject to federal appropriations and there are certain thresholds and requirements for spending grant funds.

Other ESSA Title Grants and IDEA Funding

Other federal formula grants from ESSA and the Individuals with Disabilities Education Act (IDEA) may be used to support technology use so long as it remains within the scope of the specific grant program. For example, funds could potentially be used to serve historically disadvantaged students in a schoolwide program (Title I), for personalizing professional support and learning for educators (Title II), to support English Language Learners (Title III), to provide specialized services for students with disabilities (IDEA Part B) and so forth. SBOs and CTOs will have to think innovatively about using funds while remaining in compliance with the program's scope to help finance district technology goals.

One-Time Grants, Partnerships, and Crowdfunding
Many non-profit and private sector organizations can help school districts finance IT initiatives through one-off grants or public-private partnerships (PPPs). It never hurts to reach out to community and business partners to see what opportunities are out there. Districts may also consider crowdfunding initiatives so long as proper internal controls are in place.

Sources/More Reading:

FCC: E-Rate Universal Service Program for Schools and Libraries
USAC: Eligible Services List for E-Rate
Every Student Succeeds Act: A Comprehensive Guide
Title IV-A Information About ESSA's SSAE Grant
The Journal: K–12 Grant Opportunities & Ed Tech Event Listings
Accessibility: CAST & CoSN Resources
CoSN: Center on Inclusive Technology & Education Systems (CITES)
Leading Learning That Truly Meets the Needs of Each Student
U.S. Department of Education: Dear Colleague Letter on Federal Funding for Technology
ASBO International's Crowdfunding Toolkit

"Be sure to keep your SBO/CSBO in the loop on all current major initiatives and any potential future large-scale initiatives and take it a step further by bringing them along for the entire ride moving forward including initial planning and pre-planning stages through execution of the initiative. The last thing they want is to be surprised and have to make quick funding decisions to support the CTO (if needed) on something that they are not fully onboard with or understand, so involve them early and often.

Taking your SBO/CSBO along for the entire ride of an initiative and educating them on your plan including the 'why' and 'how' will make the process much smoother, will promote transparency, and will create buy-in and ownership creating a unified front, which is very important for districts and will lead to more successful initiatives!"

—Mike Frantini, Chief Technology Officer, Community Consolidated School District 21 (CCSD21) (IL)

DATA MANAGEMENT & SECURITY

Challenge/Opportunity: A rapidly changing and increasingly interconnected world, combined with new emerging technologies and the rise of the Internet of Things (IoT), brings new threats. SBOs and CTOs must work together to protect sensitive student, staff, and other school information.

BALANCING DATA PROTECTION AND TRANSPARENCY

Given the possible serious repercussions of school data breaches, parents and other education stakeholders want assurances that data privacy is being protected.

SBOs and CTOs must work together to identify threats, develop policies and practices to protect data, and prove to the public how the district is safeguarding data. K–12 leaders must balance regulatory compliance, including transparency, when sharing data about teachers, budgets, staff, and more. Here are best practices to help make school data available and safe at the same time.

6 Safeguards to Protect School Data

1. **Know your laws and regulations.** Districts must comply with a variety of laws and regulations at the local, state, and federal levels. Some of the federal laws district leaders should be familiar with are the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Internet Protection Act (CIPA), and vendor requirements under the Children's Online Privacy Protection Act (COPPA), among others. Review compliance procedures to maintain good habits and stay informed of any changes. When in doubt, check with your legal counsel to ensure your district is in compliance.

2. **Prioritize critical data.** Critical information (e.g., personnel and payroll records, student medical histories, and other personally identifying information) must be carefully stored and securely protected. Other information that doesn't identify or relate to a specific individual, like lunch menus, graduation rates, and calendar events aren't critical and don't need to be treated the same way.

3. **Implement authentication management and regular training.** Authentication management is all about access to organizational systems and resources. The traditional approach to access control has been to assign usernames with complex password requirements. However, as the environment changes, so should the organization's security practices. According to the federal Cybersecurity and Infrastructure Security Agency (CISA), over 90% of cyberattacks start with phishing. Training staff to detect and report suspicious emails is the first and most important step in dealing with phishing.

4. **Secure storage.** As school districts rely more on technology to complete everyday tasks (e.g., learning apps, online assessments, cloud data storage, etc.), strong data security is crucial. Partner with IT staff and a trusted provider to find the safest option for your district.

5. **Schedule an audit.** The identified best practice is to conduct bi-annual security audits of systems.

6. **Consider cyber insurance.** To take advantage of breach or cyber insurance, you must meet all the conditions necessary for the payout by the insurer. No two insurance companies will have identical requirements, but there will be some common elements.

   Questions to ask:

   - What circumstances do not qualify for a payout?
   - What is the definition of real liability?
   - What is the deductible per claim? (Note that sometimes the deductibles plus premiums are more than the payout.)
   - What is the total aggregate payout? (This will often be less than the aggregate of other line items.)
   - Do any specific logging requirements exist? (E.g., active directory, financial system, successful and unsuccessful attempts, etc.)

Sources/More Reading:

CISA—Shields Up: Guidance for Families

Five Cybersecurity Safeguards for School Districts

U.S. Department of Education: Protecting Student Data Privacy

Three Things You Can Do in Less Than Three Hours of Work to Significantly Reduce Cybersecurity Risk

Cybersecurity Remains K–12 EdTech Leaders' No. 1 Priority in 2024

Top 5 Cybersecurity Threats

Authentication Management

CoSN Podcast: Cybersecurity Insurance and Risk Assessment

CoSN Podcast: The Cybersecurity Leadership Game

Proactive Leadership Regarding Cybersecurity in School Systems

Cybersecurity Incident Response: The Game

CoSN Podcast: K–12 Cybersecurity: Building Defensible and Resilient K–12 Digital Infrastructure with the U.S. Department of Education

AI & Cybersecurity: What You Need to Know

Student Data Principles to Improve K–12 Practices

SBOs and CTOs should reference these leading principles for data privacy and management to improve their district data policies and procedures. Protecting student data privacy is a critical and fundamental school system requirement. However, addressing legal requirements and community expectations for student data privacy while allowing for data-driven decision-making and technology use is a significant challenge.

CoSN's Student Data Privacy Toolkit provides the guidance you need to create and improve your student data privacy program while building confidence and trust across your community.

- Part 1: Student Data Privacy Fundamentals
- Part 2: Partnering with Service Providers
- Part 3: Transparency and Trust

DEVELOPING BETTER DATA POLICIES VIA STAKEHOLDER ENGAGEMENT

Effective transparency policies can promote better human resource management, boost student achievement, and create greater community understanding and engagement. Here are several questions SBOs, CTOs, and others should consider when developing district policies.

- Are relevant stakeholders included in the development of transparency policies?
- Are stakeholders given enough time and information to make participation meaningful?
- Are superintendents, SBOs, CTOs, and school board members on the same page? If not, can transparency measures help them get there?
- Can transparency of data collection and analysis facilitate needed benchmarking?
- Is the transparency policy designed to be useful in benchmarking with comparable districts?
- Will the district's data management software system customize school success solutions? Can it be leveraged to engage internal and external stakeholders?
- Is transparency promoted as a two-way street within the district? Are all stakeholders free to use transparent information to engage with one another and with district leaders?

Build a Trusted Learning Environment (TLE)

CoSN, ASBO International, AASA, ASCD, and 28 school systems created the Trusted Learning Environment (TLE) Seal program to help school districts build and mature organization-wide student data privacy programs. Applicants to the TLE Seal program receive assessments of their privacy materials and recommendations for improvements. Once a certain level of maturity is reached, applicants earn the TLE Seal.

The TLE Seal is the only student data privacy framework in the nation and the only data privacy seal for U.S. school systems. Earning the TLE Seal demonstrates not only a level of maturity in the school system's data privacy program but also a commitment to continuously improving and building a culture of transparency and trust with the community around data privacy practices.

Applying for the TLE Seal presents SBOs and CTOs an opportunity to collaborate on building a better relationship with their community while meeting their district's data privacy goals.

Trusted Learning Environment Mini Seals
The new TLE Mini Seal Program allows school districts across the country to earn recognition for one or more of the following practice areas as they make progress toward earning the full TLE Seal.

- Leadership Practice
- Business Practice
- Data Security Practice
- Professional Development Practice
- Classroom Practice

Sources/More Reading:

A Transparency Checklist for K–12 Administrative Software
TLE Seal Program and Resources Website
Protecting Student Privacy in a Trusted Learning Environment
TLE Self-Assessment
Student Data Privacy Fireside Chat: FERPA Solutions for Your District
Leading Effective Data Privacy Processes Within a School District Setting

PREVENTING RANSOMWARE AND OTHER CYBERTHREATS IN SCHOOLS

Ransomware is malicious software that blocks access to files or systems using encryption until the victim pays a ransom in exchange for a decryption key to unlock the files. Although ransomware isn't new, it has advanced in sophistication over the years, allowing it to spread, evade detection, and encrypt files in increasingly complex ways. CISA reports, "For K–12 schools, cyber incidents are so prevalent that, on average, there is more than one incident per school day."

How Can School Districts Protect Themselves from Data Breaches?

1. **Secure data backups.** Frequently back up data and secure files in locations not directly connected to the district's servers. Follow the 3-2-1 rule: keep three copies of data, two different types of media, and one copy off-site. Air gap data backups (an air gap data backup is a copy of data stored on a device that is completely disconnected from all networks, protecting it from online threats). Test and practice recovery of data from backups in ongoing regular intervals. Limit access to essential network drives.

2. **Use threat intelligence and event monitoring tools.** For K–12 districts, establish a baseline of normal activities to help identify deviations, use threat intelligence feeds, implement Security Information and Event Management (SIEM) tools, conduct regular cybersecurity training, develop an incident response plan, and collaborate with cybersecurity organizations. These measures help schools effectively manage cyber risks and ensure a secure educational environment.

3. **Be aware of suspicious activity.** Early detection is key to mitigating data loss. Run select backups during the day and pay attention to data storage anomalies to stay alert for an attack that has recently occurred or is actively underway.

4. **Train all users.** Educate staff and students on data security best practices (e.g., downloading software from secure/trusted sources, changing passwords, etc.). Warn users to quickly physically disconnect from the network if they suspect a virus or other threat has occurred. Establish software restriction policies to prevent the execution of malicious files in vulnerable directories.

5. **Install patches and updates monthly.** The responsibility of the K–12 educational institution is to make the physical hardware unavailable to bad actors. Patching or updating the applications that run on the physical hardware device is one way to protect the infrastructure of the institution. Install patches on time every month. Update your firewall rules to enhance security by blocking unauthorized beacons, restricting external access to critical services, limiting international communications, and monitoring all traffic for unusual patterns.

6. **Engage the experts.** Employ security experts and in training IT staff to examine systems and protocols and invest in cyber insurance. Reach out to local, state, and federal authorities early on to build relationships and establish contacts to collaborate on a cybersecurity plan. That way if something happens, you'll know who to call and be able to swiftly coordinate response with the appropriate agency to prosecute offenders and minimize district impact. Regarding ransom demands, the FBI advises against paying ransom as it doesn't guarantee decryption and may encourage further attacks. Immediate consultation with law enforcement and legal advisors is recommended.

7. **Be proactive.** Don't rush to implement IT systems and make yourself vulnerable to threats. Ensure your business and IT teams meet regularly to review security tools, processes, procedures, and internal controls to determine where improvements are needed. CTOs and SBOs can collaborate on the district's budget to procure cybersecurity safeguards as needed and prioritize IT as a strategic investment to support overarching risk management goals.

Tips for Obtaining Cybersecurity Insurance

SBOs and CTOs should work together to review and assess cybersecurity insurance options to find a plan that best meets the district's needs. In the unfortunate event a district needs to leverage its insurance plan, note that the district must meet all of the insurer's specified conditions to receive a payout. Because of the high number of cyberattacks in recent years, insurers are evaluating their vulnerability. Rates are rising and tighter controls are being put into place. Districts that do not provide sufficient documentation or that apply without the required controls might not receive coverage, may be required to pay higher premiums, or may risk having lower coverage limits for the account.

If your district is preparing to apply for or request a quote for cyber insurance, here are some recommendations to ensure you have adequate controls in place.

- Remove or reduce administrative rights to reduce the attack surface. Practice least privilege enforcement.
- Manage all privileged remote sessions from vendors and employees.
- Eliminate unsupported operating systems and platforms.
- Review the environment for indicators of compromise to confirm that none are found. If found, remediate.
- Document the steps taken to detect and prevent ransomware attacks.
- Assign someone to handle all data security.
- Conduct regular security awareness training for all employees.
- Put written information security and privacy policies in place.
- Have a tested business continuity and disaster recovery plan.
- Install antivirus and firewall systems and update them regularly.
- Stay current on updates and patches for all critical information technology systems and applications.

Sources/More Reading:

Ransomware: Holding Data Hostage

Report: Half of K–12 Data Breaches Caused by Staff & Students

Multi-State Information Sharing & Analysis Center Cybersecurity Resources

FBI—Ransomware

CoSN—Cybersecurity Response: Ransomware and Cyber Insurance Guidelines

CoSN Cybersecurity Resources

ASBO International Best of School Business Affairs Magazine: Cybersecurity Edition

DETECTING AND PREVENTING FRAUD

When fraud happens in a school district, it is a traumatic event for the whole community. An SBO's time is better spent working to minimize the risk of fraud rather than playing damage control, and the CTO can help. Prevention is important since fraud not only causes the school system to suffer financial losses, but it destroys public trust and redirects time and resources that should be spent on student learning. However, SBOs and CTOs can prevent fraud if they understand the conditions in which it is likely to occur, as illustrated below.

Fraud can be detected via employee or anonymous tips, internal/external audits, internal controls, by accident, and by local authorities. Forensic auditing techniques and software can be strong fraud countermeasures since they can mine and analyze data to catch double payments, suspicious vendors, numbering gaps or duplicates, and outlier data. SBOs and CTOs can identify the right software and initiate steps to reduce fraud opportunities by strengthening internal controls, setting up safeguards for authorizing and approving transactions, and securing financial assets and records.

Sources/More Reading:

Understanding, Detecting, and Preventing Fraud

Adding Data Mining and Analytics to Your Toolbox

CREATING CYBER-PHYSICAL SECURITY SYSTEMS (CPSS) IN SCHOOLS

In the wake of school violence, bullying, and other safety threats, school districts are turning to technology to secure campuses with Cyber-Physical Security Systems (CPSS). CPSS bridges physical and digital environments and may include anything from entryway cameras and automatic locks to intercoms, facial recognition software*, and biometric readers. They can be integrated into security platforms for automatic threat detection and facility lock-down, remote video observation through web-enabled camera systems, and enhanced communications with stakeholders and first responders. These tools frequently depend upon network infrastructure to function and must be architected to work within their segment of the network for security.

Here are examples of tools districts use in support of CPSS:

- Access controls—locks, gates, vestibules, metal detectors, door barriers, entry cards, access software, facial recognition software, and central lockdown capability.
- Surveillance—cameras, live video feeds, body-worn cameras, and other monitoring tools. All devices with network cables must be hidden and inaccessible or it contributes to the problem.
- Communications equipment and platforms—wired/wireless communication technologies, intercom systems, local alarm communicators, phone systems, two-way radios, enhanced 911 communications, and attendance and check-in apps.
- Sensors and alarms—mapping and verification solutions, duress alarms/panic buttons, door and window sensors, gunshot detectors, robots, and lighting.
- Fogging and pepper spray systems—smokescreens, chemical aversives, etc.

SBOs and CTOs can work together to build these systems and determine their impact on physical facilities, network infrastructure, and district procedures and policies as part of their broader school security strategy. Two issues to consider are 1) the potential legal impact these technologies may have on student privacy and civil rights and 2) the network burdens a new CPSS can put on the district to successfully utilize it.

(*Caution: Facial recognition technology can be biased and should be tested rigorously.)

Sources/More Reading:

The Latest in Video Surveillance: Increasing School Security Campuswide

What are Cyber-Physical Security Systems?

ASBO International's Best of School Business Affairs Magazine: Cybersecurity Edition

"Sometimes people think of IT as really being either devices (computers, iPads, Chromebooks) in the hands of staff and/or students, or infrastructure including servers and networking. It's worthwhile for SBOs to meet with their IT counterparts to talk more expansively about roles, responsibilities, and scope. Copiers may be all IT, all business offices, or some overlap. It's not common that they do not involve at least some basic amount of networking or connectivity. Physical security (not just email/phishing/etc.) often involves some technology, whether that's how doors lock or release, video cameras, or something else. Talking about who takes the lead and how the groups work together can help avoid missing things or compromising systems.**"**

—David Bein, PhD, SFO, Past President, Illinois Association of School Business Officials; Retired School District Chief School Business Official (IL)

IT INFRASTRUCTURE & SYSTEMS MANAGEMENT

Challenge/Opportunity: Technology is everywhere—we rely on it for nearly everything. And, as Internet connectivity becomes increasingly essential to school district operations and classroom instruction, SBOs and CTOs should work together to meet rising demands for digital devices and 24/7/365 access to learning. They also need a backup plan for when things go wrong.

LEVERAGING CLOUD COMPUTING TO SUPPORT K–12 OPERATIONS

Cloud computing can be a game changer for district operations and education service delivery. CTOs can help SBOs understand the potential benefits of cloud computing and considerations when investing in this solution for operational and educational challenges.

What Is Cloud Computing?

Cloud computing encompasses computing services managed or hosted by another supplier that provides convenient, on-demand access to networks, servers, storage, applications, and services. These resources are quick to set up with minimal management/service provider interaction and do not require major up-front capital investment. There are three models: Infrastructure, Platform, and Software as a Service (IaaS, PaaS, and SaaS), which are defined by several characteristics:

1. **On-demand self-service.** Users can access computing resources whenever they need them.
2. **Broad network access.** Users can access capabilities with a variety of devices.
3. **Resource pooling.** Cloud service providers leverage economies of scale by making shared resources available across customers in multi-tenant models.
4. **Rapid elasticity.** Resources are delivered quickly according to the user's capacity requirements.
5. **Measured service.** Usage is monitored, controlled, and measured for billing, reporting, and managing.

Cloud Computing: Benefits & Considerations

- Cloud computing offers great advantages for understaffed districts and districts looking to save money. CTOs who pursue this approach need to examine data transit fees. This is usually not a problem with SaaS solutions but can become a burden with IaaS and PaaS solutions where data transit can drive up costs.

- It is often less expensive than doing the services in-house, since the hardware and levels of application support move from the district to the vendor.
- The district will still need to administer the application, manage the service provider, and pay operational fees, but no expensive capital investment in server hardware is required. The benefit of this is that it moves a lot of expenses from capital expenditures (CapEx/CapX) to operating expenditures (OpEx/OpX) in budgets, making budgets flatter and more manageable.
- Cloud computing offers a possible solution to rising student and staff demand for 24/7 mobile application and digital content access when lacking internal district support capabilities to meet demand.
- It can help IT staff offload some server- and application-specific support requirements.
- It still requires districts to address/safeguard data security, privacy, and identity management.
- Districts must ensure their Internet and internal network bandwidth can accommodate data transmission loads and extra bandwidth needed for responsiveness, backup, and recovery.

As districts adopt these services, SBOs and CTOs can work together and find solutions for managing subscription costs, maximizing feature utilization and effectiveness, and reducing duplicative services.

Sources/More Reading:

Cloud Computing

IMPROVING K–12 INTEROPERABILITY

Interoperability has the potential to transform teaching and learning. CTOs can help SBOs understand its potential benefits and the financial and staff support required to implement it fully.

Interoperability is the capacity of different technologies and educational systems (e.g., Student Information, Enterprise Resource Planning, and Learning Management Systems) to work together securely and seamlessly to exchange data effectively. Interoperability promises to transform teaching and learning by giving teachers, learners, and administrators more access and control. The benefits of interoperability on day-to-day school district operations and database decisions are increasing; districts that find ways to harness this power can better serve their students.

Education decision-makers must lead efforts to select products that not only meet their immediate teaching, learning, and administrative needs but also support standards-based data integration as a technical requirement. Products developed with proprietary methods "don't play

well with others" and can cause more harm than good if data can't be shared easily between systems.

The growing demand for sophisticated analytics, accountability reporting, and performance management tools requires data exchange between systems. Together, SBOs and CTOs seek to build tools that use content and data assets strategically across several systems and assemble solutions that enable staff to make data more meaningful and understandable.

3 Key Areas to Enhance Interoperability

1. **Digital Learning Resources.** Digital learning environments require high levels of interoperability between digital learning resources, applications, and the networked computing infrastructure of an educational enterprise. Thus, educational resources increasingly are developed with the presumption that they will be integrated into multiple enterprise service environments that include both new and legacy content/ systems.

2. **Learning Data Exchange and Outcomes.** The main objective of data connectivity standards is to provide universal connectivity to data sources from a variety of platforms, using a standard set of commands to transfer data efficiently and cost-effectively. Data connectivity is essential for mission-critical applications including enterprise resource planning (ERP), student information systems (SIS), learning management systems (LMS), and data warehouse applications.

3. **Identity Management (Authentication and Authorization).** Poorly implemented or maintained Identity management processes are a key vector used by cyber criminals to attack school districts' data environments. Identity Management helps control who can access what information within an organization and ensures that sensitive information is protected and only available to the right people.

   This includes the following:

   - Managing the process of creating and deleting user accounts.
   - Setting up and managing passwords.
   - Assigning and revoking permissions for different systems and applications.

   The goal of identity management is to ensure the security of information and systems while making it easy for people to access the resources they need to do their jobs.

Strategic approaches to interoperability are increasingly important in education because all systems and platforms must work together to seamlessly deliver services across the district. When systems work well together, so will the district's ability to collaborate, cut costs, improve security and privacy, drive transformation, and serve customers efficiently. To achieve effective interoperability, districts must agree on standards for procuring systems and platforms, which presents another opportunity for SBOs and CTOs to work together.

Sources/More Reading:

An Introduction to Interoperability

CoSN Interoperability Toolkit

How to Not Invest in Data Management Systems

Project Unicorn: Interoperability Crash Course & Tools

MAINTAINING CONTINUITY DURING A DISASTER

SBOs and CTOs must be prepared for any emergency that can impact technology operations, whether it be a hurricane, earthquake, or something else. Before a disaster strikes, districts must be ready to assess damage, bring critical systems back online, update stakeholders, and resume operations. They should collaborate on a Business Continuity Plan (BCP) for any emergency. School districts are expected to maintain written policies for disaster recovery and business continuity. These policies should be reviewed and updated regularly.

How to Develop a Disaster Preparedness Plan for Any Situation

1. **Form a disaster preparedness team.**
    - Include Operations, IT, Instruction, local and federal emergency management, and key vendors.
    - Initiate a Business Impact Analysis (BIA): Charge the committee with identifying potential threats, and with formulating, disseminating, and executing the disaster preparedness plan in the event of an emergency.
    - Create a comprehensive communication strategy detailing the protocols to be followed before, during, and after a disaster, while clearly outlining the roles and responsibilities of team members in managing and distributing information.
    - Ensure this team also focuses on the cybersecurity aspects of disaster preparedness. This includes identifying digital assets and protecting them against potential cyber threats in alignment with the NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), a U.S. government agency.
2. **Ensure the team prepares a comprehensive emergency plan for different types of disasters.**
    - Develop dynamic response protocols that can be adapted based on the nature of the disaster, whether it's a cybersecurity incident, natural disaster, or pandemic. This includes specific IT incident response teams and protocols.
    - Focus on technology's role in providing continuity during disaster preparedness (e.g., for instructional activities, data/record keeping, assessment and accountability, and internal and external communication with stakeholders).

- Enterprise Incident Response: Ensure the plan accounts for personnel, facilities, hardware, software, and critical communication resources, and prioritizes which systems should be protected first. This plan includes identifying Recovery Time Objectives (RTO), or the maximum amount of time acceptable to restore a system, and Recovery Point Objectives (RPO), or the maximum amount of data the organization can lose in the restoration process.

- Ensure that plans include flexibility and scalability, which can help accommodate various scenarios and ensure quicker service restoration.

3. **When developing a disaster preparedness mitigation plan, at minimum, the plan should:**

   - Identify preventable vs. unavoidable disasters and address what can be done to eliminate or reduce the likelihood of the disaster and its impact.

   - Ensure alternative communication pathways have been defined for all BIAs.

   - Ensure there are accurate site maps for each facility. Clearly label all rooms in buildings with the room numbers inside and out.

   - Ensure all servers are protected from physical disruptions (e.g., water damage, tampering, etc.) and are routinely backed up. Incorporate systematic detection mechanisms for IT disruptions or unauthorized access during a crisis.

   - Include a detailed training plan for all personnel on disaster response procedures including scheduling drills and simulation exercises (tabletop tests) on a regular schedule. Debrief and improve your plan after these events.

4. **Think through all processes, people, and procedures to guarantee district preparedness.**

   - Detailed planning, redundancy in personnel and equipment, and drills and practices for preparation and response are key to efficiently restoring critical operations.

   - Build a schedule of regular reviews and updates to the plans based on new threats, technological advances, and lessons learned from drills and actual incidents.

Sources/More Reading:

IT Crisis Preparedness Countdown

At the Ready: Planning for Business Continuity

Disaster Preparedness

INNOVATION IN TECHNOLOGY & EDUCATION

Challenge/opportunity: New advances in technology and increasing interconnectivity require students to learn new skills to be successful and competitive in the global economy. SBOs and CTOs must work together to provide educational programs and services that prepare students for their future careers.

ADAPTING TO NEW TRENDS AND DRIVING INNOVATION IN EDUCATION

SBOs and CTOs must stay ahead of rapidly changing trends in education to ensure students graduate and can succeed in today's world. District leaders must be aware of key drivers of change that define and dominate local and global demands for labor so that students learn the professional skills they need. SBOs and CTOs must shift from a reactionary to a proactive mindset to drive change in their communities. Identifying what drives, hinders, and enables innovative teaching and learning in schools can help districts implement strategies to positively manage and lead change.

CoSN advances K–12 technology integration through annual trend reports, one of which is the "Driving K–12 Innovation Hurdles, Accelerators, and Tech Enablers Report." This report is shaped by insights from a global advisory board of over 100 K–12 leaders and changemakers and analyzes key trends affecting educational technology. Findings are released early each year, providing CoSN members and partners with critical data to enhance learning environments. Here are key trends for innovation in education from CoSN's 2024 report.

Top 3 Hurdles for K–12 Innovation

1. **Attracting and Retaining Educators and IT Professionals.** Hiring and keeping school staff is a significant problem for school systems; many educators are experiencing social and emotional burnout, as well as low pay compared to other sectors, causing them to set aside their passion for teaching and leave the field. Educators also face a lack of trust and respect from society and systems—trust that teachers know what they are doing and have the best interests of their students at heart. For IT Professionals, there are the added stressors of industry comparison, as many private companies can offer higher salaries, flexible work schedules and locations, and more time off.

2. **Ensuring Cybersecurity and Safety Online.** Teaching, learning, and conducting business in education online is now a baseline requirement for teachers, students, and administrators. Yet there is a lack of trust that the K–12 ecosystem and learning environments are safe and secure. Schools must be proactive in building systems to protect every user, at every level, in every technology system, in every application, and in every workspace—home or school, 24/7. The risk is intensified as technology needs grow, new cybersecurity threats continuously enter the landscape, and malicious actors

get smarter. Schools are expected to keep up with these risks while increasing protection measures, employing qualified staff, and raising industry standards to strengthen the safety and security of the online world. To effectively manage this risk is costly, but it is non-negotiable.

3. **Scaling and Sustaining Innovation.** Whether it be practices for effective teaching and learning, organizational business processes, or technology usage, schools are challenged to engage in and effectively scale innovation—adapting what is working well and scaling it out across a school, district, or state/country. Four years after the COVID-19 pandemic began, the education system we once knew has experienced seismic opportunities for change; yet, in many school systems and parts of society, there is still a desire to pull back to the familiar pre-pandemic education models. This highlights an inertia in education that resists change: a complex system that reinforces past practices and discourages innovation. This hurdle reflects both the resistance to change that is present within many schools, and the deeply rooted education and social systems that exert pressure against change, as well as the need to expand what is working to a larger scale.

Top 3 Accelerators for K–12 Innovation

1. **Changing Attitudes Toward Demonstrated Learning.** There is a rising groundswell of discussion around assessing, documenting, communicating, and assigning value to student learning—as well as relating this learning to higher education, vocational training, and career pathways. This complex issue is intertwined with discussions of learner agency and personalization, the value of the experience and social aspects provided by education institutions, student trajectories through and beyond K–12 systems, and the relationship between learning, lifelong learning, and careers.

2. **Building the Human Capacity of Leaders.** Strengthening the professional community of schools and providing opportunities for educators and all K–12 professionals to learn and master new skills can open the door to innovative practices that can enhance student experiences. When schools invest in their staff by providing opportunities to gain and improve upon skills, to exercise agency in their work, and to make mistakes without fear, they create an environment that attracts innovative people.

3. **Learner Agency.** It's all about students as leaders in their learning; reconceptualizing their role from that of "student" to that of "learner." When immersed in a strong learning environment, learners could transform from order-takers to innovators, experience the state of flow, and learn far more authentically. For schools to facilitate "learner agency," they must also encourage "educator agency." Learner agency is essential for lifelong learning and requires a different approach to school structure and practices. Truly embracing learner agency will require transforming education systems.

Top 3 Tech Enablers for K–12 Innovation

1. **Generative Artificial Intelligence.** Artificial intelligence (AI), the ability of machines to perform tasks that are typically associated with human intelligence, such as learning and problem-solving, has been around for decades. Generative AI (Gen AI) refers to a type of artificial intelligence system designed to generate new content such as

text, images, audio, or video in response to user prompts. Unlike other AI systems that focus on pattern recognition or classification, Gen AI can create new and original content that closely resembles human-created content. Generative AI has emerged as a transformative force in education, changing both how students learn and what they need to learn. As school systems worldwide explore the benefits and challenges of this technology, they are both developing and seeking expert guidance to meet the urgent need for policies and processes that ensure the safe, effective, and responsible use of Gen AI for all stakeholders.

2. **Analytics and Adaptive Technologies.** These are digital technologies that collect and use data related to teaching and learning. Analytics refers to the process of analyzing data collected about student learning and the opportunity to leverage data to inform instructional decision-making. Adaptive technologies are tools that adapt to the student based on their interactions with the technology, changing the pathway provided according to user need and/or interaction. These adaptations could be in the form of suggesting next steps, providing remediation, controlling pacing, or providing feedback based on analysis of the student's performance. Adaptive technology is broader than assistive technology for accessibility-supporting technology and can be beneficial for all students.

3. **Rich Digital Ecosystems.** Connecting systems or digital environments can form powerful digital ecosystems to enable student learning and/or support education administration. These interconnected systems of online and virtual spaces can span formal school settings and beyond.

TIP: Discuss these questions with your team to assess your district's preparedness for the future.

- What is the impact of the trends mentioned above on your school district? How are these advances in technology affecting the way educators teach, and students learn?
- How well is your school district preparing for and adapting to these changes? Where has the district been successful? Where is there room for improvement?
- How will the district work together as a team to accommodate these trends?
- How will the district engage teachers, parents, students, and the community throughout this process? Is it helpful to invite neighboring school districts, businesses, nonprofits, or professional associations to engage on these issues?
- What other shifts, changes, or trends do you foresee that will impact education? How will your school district prepare for them?

Sources/More Reading:

Driving K–12 Innovation
Accelerating Innovation: A Guide to Leverage the 2024 Driving K–12 Innovation Report
CoSN AI Resources
K–12 Generative AI Readiness Checklist
CoSN/CGCS K–12 Gen AI Maturity Tool
Teach AI Toolkit

GENERATIVE ARTIFICIAL INTELLIGENCE (GEN AI)

SBOs and CTOs are tasked with the challenge of balancing fiscal responsibility and educational innovation. In today's rapidly evolving technological landscape, Generative AI (Gen AI) stands out as a transformative force that promises to revolutionize how we teach and what students need to learn. By strategically investing in this technology, education leaders can position their school districts at the forefront of educational innovation while potentially realizing significant long-term cost savings and operational efficiencies.

The value of adopting Generative AI isn't just for the sake of staying current; it is also about preparing students for a future where AI will be ubiquitous in the workplace and daily life. Moreover, it offers an opportunity to address persistent challenges in education, such as personalized learning and administrative inefficiencies, in novel and effective ways. Given this, SBOs and CTOs need to work together to discuss and plan a path forward for Generative AI investment.

Justifying Gen AI Investments in the Budget

From a financial perspective, the initial investment in Generative AI may seem substantial. However, when viewed through the lens of long-term benefits and potential cost savings, it becomes clear that this is a prudent allocation of resources. Here is an example of key areas of investment and their rationale.

1. **Technology Infrastructure:**
    - Initial investment: 2–5% of the annual budget.
    - Annual maintenance: 0.3–0.5% of the annual budget.

    Rationale: A robust technological infrastructure is the foundation upon which all AI initiatives will be built. This ensures equitable access and sets the stage for future innovations.

2. Curriculum Integration:

- Development costs: 0.5–1.5% of the annual budget.
- Annual updates: 0.2–0.5% of the annual budget.

Rationale: Integrating AI into a district's curriculum isn't just about using new tools; it will prepare students for an AI-driven future, enhancing their critical thinking and digital literacy skills.

3. Personalized Learning:

- AI tutoring software and data analytics tools: 1–2% of the annual budget.

Rationale: AI-driven personalized learning can significantly improve student outcomes, potentially reducing the need for costly remedial programs in the long term.

4. Administrative Efficiency:

- Investment in AI for administrative tasks: 0.5–1% of the annual budget.

Rationale: By leveraging Generative AI for tasks such as scheduling, report generation, and data analysis, the district can significantly reduce administrative workload. This will cut costs and allow staff to focus on higher-value activities that directly impact student success.

5. Long-Term Cost Savings and Sustainability:

- Projected savings in textbooks and materials: 3–5% of current spend.
- Potential reduction in remedial program needs: 1–2% of current spend.
- Administrative cost reduction: 2–3% of current administrative costs.

Rationale: While the initial investment is significant, the long-term savings across multiple areas justify the expenditure. Moreover, these savings can be reinvested into further innovations, creating a cycle of improvement.

By adopting Generative AI, a district is not just implementing new technology; it is fundamentally transforming its educational model to create more engaging, personalized learning experiences for students while simultaneously streamlining operations and reducing long-term costs.

SBOs and CTOs must ensure that the district is financially stable and prepared for the future. Investing in Generative AI allows a district to fulfill both of these obligations, positioning its schools as innovative leaders in education while maintaining fiscal responsibility. This strategic investment is more than an expense—it's an investment in students' futures and the long-term success of educational institutions.

Note: These percentages are simply examples but are intended to be significant enough to drive meaningful change and encourage a district to make substantial investments in Generative AI. Percentages may need to be adjusted based on the district's size, current technology integration levels, and unique needs.

PREPARING FOR THE IMPACT OF NEW TECHNOLOGY IN SCHOOLS

Education technology can be a powerful tool—if your infrastructure can handle it. SBOs and CTOs must consider how changes in teaching and learning will affect demands on school infrastructure so that when it's time to take the digital leap, the district will be ready. Here are several things to remember:

- As technology programs grow, new grade levels will be added, and more schools will come on board. This means more students will bring their devices and put pressure on networks.
- Education content is changing. Digital curriculum is getting larger, requiring more bandwidth to transfer lessons onto student devices. Devices also need to sync with cloud computing systems, making them "chattier" as they send data across networks. Even simple web pages have more content, which requires more bandwidth for web browsing.
- As teaching and learning with technology matures in the district, there is usually a shift to more student-centered/personalized learning. Anticipate increased student Internet usage, demand for digital resources, and use of online learning communities for students and staff.
- Districts may need to do a cost trade-off analysis to determine the best ways to connect schools to the Internet, via "lit" and "dark" fiber networks that are ISP-owned, school leased, or created from scratch. The trade-off costs between taking on operations and maintenance versus being beholden to a single provider must be considered carefully, but there are opportunities for reducing costs via taking control of the district's Wireless Access Network (WAN).

Sources/More Reading:

Will Transformed Teaching and Learning Break Your Network?

CoSN's Digital Leap Success Matrix

CoSN Networking and Systems Design

Empowering School Districts: An Introduction to AI Use Policy Toolkit for Education

Recommendations from CoSN's Driving K–12 Advisory Board

1. Build Off What We've Learned During the Pandemic.

"As educators, we need to transfer all the good we know about when and how and why students learn then integrate this educative capability within the connective capability of the technology tools. The question is how do we combat the inertia of returning to pre-existing practices once back in the classroom in order to leverage the best of both learning worlds—our expertise in pedagogy plus the mass availability of personally owned devices?"

—Karen Swift, Head of Department – Business and Technologies, James Nash High School, Queensland, Australia

2. Use Pedagogy Strategies to Personalize Learning.

"To realize a vision for personalized learning, instructional practices should be targeted and relevant (i.e., differentiated, culturally responsive, adaptive, standards-aligned, etc.), actively engaging, socially connected, and growth-oriented. While personalization may manifest in different ways within different contexts, this constellation of strategies holds constant."

—Beth Holland, Ed.D., Research and Measurement Partner, The Learning Accelerator, USA

3. Leverage Learning Resources to Personalize Education.

Consider using online learning resources as a strategy to personalize and individually pace learning. Whether students are learning in the classrooms or remotely, 1:1 devices allow educators to individualize the pace of learning for their students in ways that they never could before.

Sources/More Reading:

Technology's Key Role for Personalization Differentiation

3 Things to Consider When Designing Digital Learning Experiences

Will, Skill & Thrill: How Learner Agency Can Accelerate Innovation

Driving K–12 Innovation: 2022 Hurdles and Accelerators

The Innovation Code: The Creative Power of Constructive Conflict

APPENDIX

ACKNOWLEDGMENTS

ASBO International and CoSN would like to thank the following individuals who contributed to this toolkit and its supplemental resources.

Stephen Agyei-Mensah, EdD, RHIT, CETL, Coordinator of Technology, Worcester County Board of Education (MD)

Linnette Attai, Project Director, CoSN Student Data Privacy Initiative and the Trusted Learning Environment Program; President, Playwell, LLC (NY)

David Bein, PhD, SFO, Past President, Illinois Association of School Business Officials; Retired School District Chief School Business Official (IL)

Keith Bockwoldt, Chief Information Officer, Hinsdale Township High School District 86 (IL)

Melissa Fettkether, Director of Business & Finance/School Business Official, Postville Community School District (IA)

Mike Frantini, Chief Technology Officer, Community Consolidated School District 21 (CCSD21) (IL)

Beth Holland, EdD, Managing Director of Research, Measurement & Policy; The Learning Accelerator, National, U.S. (RI)

Anton Inglese, PhD, SFO, CETL, Chief Financial Officer, Batavia Public School District 101 (IL)

Frankie Jackson, RTSBA, CETL, Trusted Technology Thought Partner and Former School District Chief Technology Officer (TX)

Suzanne Jones, Retired School District Management Information Systems Coordinator (MD)

Pete Just, CETL, Project Director, CoSN AI; Executive Director, Indiana CTO Council (IN)

Jennifer Lotze, CETL, Cybersecurity State Coordinator, Region 5, CISA; Former District Instructional Technology Leader (MN)

Paula Maylahn, Project Director CoSN Interoperability Initiatives; Paula Maylahn Consulting (NJ)

Amy Mclaughlin, MS, MA, CETL, CISM, CHPS, CDPSE, CISSP, Project Director, CoSN Cybersecurity and Network & Systems Design Initiatives Project; Executive Director, Technical and Solutions Architecture, Oregon State University (OR)

Lenny Schad, Co-Founder K12 Strategic Technology Advisory Group (FL)

Josh Stephenson, Chief Financial Officer / Treasurer, Hinsdale Township High School District 86 (IL)

Karen Swift, Head of Department, Business and Technologies; James Nash High School, Queensland (Australia)

Elleka Yost, MA, Director of Advocacy & Research, Association of School Business Officials International (ASBO) (VA)

DISCLAIMER

The content in this toolkit does not reflect any official endorsement of a specific technology vendor, service, or practice by ASBO International or CoSN, their officers, affiliates, or members. This toolkit is not intended to provide or supplant specific legal, IT, or financial advice. Please consult with your school system's counsel for specific questions dealing with your district's circumstances.

CONTACT US

Do you have another idea or resource that can help school business and technology leaders work better together in education? Contact us today!

ASBO International:

Call 866.682.2729 or email asboreq@asbointl.org.

CoSN:

Call 202.558.0059 or email membership@cosn.org.

ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

CoSN Leading Education Innovation