The Blueprint for Building a Scalable, Sustainable, and Learner-Focused Infrastructure in Your District

The COVID-19 pandemic forced school districts nationwide to pivot overnight to virtual learning. School districts rapidly purchased and deployed thousands of devices, hotspots, and digital tools to facilitate virtual learning for all students and staff. With the high demand for resources to meet the logistics and support needed for deployment, technology and curriculum staff were not only stretched thin, but significant gaps in the accessibility, resiliency, and security of educational technology ecosystems quickly became apparent.

According to the "The State of K-12 Cybersecurity: 2020 Year in Review" report published by the K-12 Cybersecurity Resource Center, "[T]he 2020 calendar year saw a record-breaking number of publicly-disclosed school cyber incidents. Many of these incidents were significant: resulting in school closures, millions of dollars of stolen taxpayer dollars, and student data breaches directly linked to identify theft and credit fraud."

As students return to the classroom, now equipped with devices they most likely did not have pre-pandemic, districts need to ensure they have the technology infrastructure in place to effectively and safely support the increased demand for virtual learning both on and off campus. In addition to learning going virtual, district operations went virtual as well. This blueprint outlines the critical components, features, and services districts may want to consider implementing in order to cultivate a safe, accessible, and user-centric K-12 digital ecosystem to support the mission and business of education.

CONNECTIVITY

The connection is everything. Without reliable, fast, and secure Internet access, digital learning and district operations will fail. School districts are looking beyond bandwidth and are thinking in terms of optimization rather than numbers. Outlined below are key features and services districts should consider when formulating their districtwide network plans and seeking out new connectivity services.

Internet Access Connectivity

- **Experience:** Leverage an experienced K-12 managed service provider who can proactively monitor, identify, and resolve network issues to supplement your technology team and enable your staff to focus on other priority projects.
- **Features and Support:** Review a provider's feature-set to ensure it includes features that will improve your network's security and performance. Example features include domain name service (DNS) resolution, DNS record hosting, real-time DNS blacklist, mail scrubbing, 24x7x365 live customer support, and remote-triggered distributed denial of service (DDoS) attack traffic blackhole routing (this last feature helps to prevent disruptions caused by students who pay for bot attacks on your network, often to avoid tests).
- **Resiliency:** Confirm that your service provider uses diverse infrastructure via numerous high-bandwidth connections to eliminate single points of failure and offer your school district reliable Internet access.

Wi-Fi

- **World-Class Engineering:** Leverage an experienced provider who has the engineering expertise required to design and install a fast, reliable Wi-Fi network customized to your unique environment and your community's needs.
- **Features:** Review a provider's features to ensure they can help you achieve essential objectives, including contact tracing, real-time data analytics, and scalability.
- **Support:** Verify that your provider offers live, 24x7x365 customer support so that learning and operations can resume very quickly in the event of an outage.

Wide Area Network (WAN)

- **Scalable:** Invest in a WAN that can be scaled up without escalating costs. An all-inclusive managed service takes the burden off the school district and eliminates costly infrastructure-associated expenses as bandwidth requirements shift. Partnering with a service provider that can offer diverse technology options, including dark and lit fiber, allows you to leverage a mix of available technologies to meet your specific community needs and deploy a flexible and scalable network.
- **Features:** Review a provider's features and contracts to ensure they manage and provide end-to-end service, including the management of all network equipment and hardware, for the entire life of the contract.
- **Support:** Select an experienced vendor that understands your unique challenges and objectives and provides 24x7x365 proactive network monitoring, maintenance, engineering, and live customer support.

Private Long-Term Evolution (LTE) Network

- **Universal Connectivity:** Bridge the digital divide and close achievement gaps by delivering ubiquitous connectivity to your entire community. Private LTE networks provide Internet access broadly accessible throughout a defined community using a band of radio-frequency spectrum such as Citizens Broadband Radio Service (CBRS).
- **Sustainability:** Build a long-lasting, sustainable, and managed private LTE network that frees IT staff from having to replace, manage, repair, and track thousands of hotspot devices that have monthly recurring subscription costs.
- **Support:** Ensure that your solution is flexible, scalable, and seamlessly integrable with your existing WAN and Internet access. Make sure your provider offers 24x7x365 ongoing network monitoring, maintenance, troubleshooting, and support.

Hotspots

- **Access:** Deliver Internet access to staff and students outside the classroom using carrier-neutral hotspots.
- **Security:** Keep students safe by selecting a provider that offers education filters compliant with the Children's Internet Protection Act (CIPA) and tracks the usage of each device.
- **Reliability:** Choose a hotspot vendor that delivers robust and reliable Internet access in your geography to eliminate frustrations and help ensure your students are using their assigned digital learning tools.

SECURITY

Cybersecurity is one of the most critical issues facing today's school districts. Failure to put systems and tools in place to protect critical, personal data can have severe, costly, and long-lasting consequences. While there is no single security solution that can offer total protection, adopting a layered security approach can help keep your education community safe against an evolving and proliferating array of threats.

Firewall

- **Expert Design:** Confirm that your firewall spares your Internet access circuit from unwanted traffic and attacks to safeguard network performance.
- **Scalability:** Select a provider that can quickly scale up your firewall to meet demand.
- **Flexibility:** Understand that your district's firewall needs can rapidly change, so choose a provider that can help you swiftly make rule changes, additions, and modifications.

Unified Threat Management

- **Security:** Consolidate multiple security and network capabilities into a single co-management and reporting service. This unified threat management will simultaneously simplify and enhance your security architecture.
- **Features:** Review your provider's service offering to ensure it includes critical features such as geo-blocking policy making, intrusion protection, malware protection, application awareness, and real-time dashboards that enable you to see what is happening on your network to identify trends and quickly resolve network issues.

Endpoint Protection

- **User Experience:** Promote peace of mind among users and IT staff with endpoint protection powered by artificial intelligence (AI) with real-time detection.
- **Security:** Ensure your endpoint protection is adaptive and equipped to handle your district's evolving security needs. This helps prevent ransomware attacks, which are more frequently targeting K-12 schools because of student data's high value.
- **Expertise:** Select a reputable and robust endpoint protection service that neutralizes attacks before they threaten your security.

Security Assessments

- **Expertise:** Engage experienced outside security experts to evaluate and perform penetration tests on your network to identify unknown vulnerabilities in your security strategy.
- **Response:** Select a security assessment provider who provides you with a thorough list of your district's potential cybersecurity vulnerabilities as well as recommendations and suggested next steps to better protect your district from cybersecurity threats.
- **Compliance:** Validate that your district's cybersecurity efforts meet compliance requirements, and identify additional cybersecurity training needs for your staff.

Layered Backup Strategy

- **Mitigation:** Regularly back up your data in the event of an attack. Keeping your data in the cloud will simplify the restoration process after an attack.
- **Secure:** Employ virtual servers for off-site data backups and select a provider with an advanced encryption standard (AES), such as 256-bit data encryption, to ensure security and data privacy in transit and at rest.
- **Cost:** Select an experienced provider who offers flat-rate pricing to ensure you have the secure backups you need at a price you can afford.

Network Segmentation

- **Design:** Proactively prevent ransomware and malware attacks from proliferating across your entire network by segmenting network components from each other for greater control and security.
- **Support:** Leverage an experienced and knowledgable service provider to design, build, and provide ongoing 24x7x365 management services for this hybrid firewall design.

Student Data Privacy

- **Discover:** Identify the apps and digital tools students are using on their school devices both inside and outside the classroom using a data analytics tool that shows your district's application usage and engagement data at the district, school, class, and student levels.
- **Evaluate:** Leverage a data analytics tool that provides privacy badging services from reputable organizations like the Student Data Privacy Consortium and IMS Global to quickly determine which apps and digital tools may pose a threat or do not comply with state and federal privacy laws as well your district's student data privacy policy.
- **Communicate:** Generate a list of approved apps and digital tools for your staff, students, and parents and broadly circulate it for transparency and to better protect student data.

COMMUNICATIONS

Effective communications are critical. Today's districts need to look beyond basic dial tone service and think of their phone system as a comprehensive onsite and mobile communications platform that enables real-time collaboration and plays an integral role in campus safety.

Cloud-Based VoIP

- **Reliability:** Review your provider's voice network architecture to ensure it is built for optimal reliability and delivers a 99.999% uptime SLA. Confirm their platform is using carrier-class equipment, is geographically resilient, uses highly-secure carrier facilities, has multiple built-in redundancies, and provides site survivability options.
- **Features:** Review the provider's voice feature-set to ensure it includes features that will lessen your admin load and enhance campus safety and security. Example features include automatic call distributor (ACD), call jump, auto attendant, hunt/rollover groups, E911, find-me/follow-me, voicemail transcription, and more.
- **Support:** Leverage an experienced K-12 managed service provider who you can rely on before, during, and after service deployment with world-class, proven customer care. Key metrics to evaluate include average hold time to reach a service technician, first contact resolution, the quality of voice engineers on staff, and the vendor's NPS score to assess customer loyalty.

Unified Communications (UCaaS)

- **Mobility:** Confirm your service provider has mobile and desktop apps that enable teachers and staff to collaborate on any device from anywhere with messaging, video, and phone calls. This not only ensures staff remain reachable any time they're away from their desks, it also prevents personal cell phone numbers from being exposed externally and can serve as a critical lifeline in emergency situations by leveraging cellular and Wi-Fi connectivity to make and receive calls.
- **Messaging:** Confirm your service provider's platform can support one-to-one messaging, integrated presence or availability status, and SMS text messaging.
- **Web Conferencing:** Leverage a service provider that has a secure, HD video conferencing and meetings platform with a variety of collaboration features. Example features include screen sharing, in-meeting chat, file sharing, whiteboarding/annotation, breakout rooms, meeting recording, and more.

Fax

- **Reliability:** Confirm your service provider can deliver a highly reliable, carrier-grade fax experience ensuring minimal to no service disruptions.
- **E-Fax:** Review your service provider's e-faxing options and whether their platform supports faxing on the go via computer, mobile device, or secure fax web portal.

FUNDING

Budgets are always tight in education, but fortunately, many of the above listed services are eligible for federal stimulus funds, including CARES (ESSER I and GEER I), CRSSA (ESSER II and GEER II), ARP (ESSER III), and ARP Emergency Connectivity Fund.

K-12 EDUCATION STIMULUS FUNDING

Eligible Services	CARES Act ESSER I $13.2 Billion MORE INFO	CARES Act GEER I $3.0 Billion MORE INFO	CRRSA ESSER II $54.0 Billion MORE INFO	CRRSA GEER II $4 Billion MORE INFO	ARP ESSER $122.8 Billion MORE INFO	ARP Emergency Connectivity Fund $7.2 Billion MORE INFO
CONNECTIVITY						
Private LTE	✓	✓	✓	✓	✓	✓*
Internet Access	✓	✓	✓	✓	✓	
WAN	✓	✓	✓	✓	✓	
Managed Wi-Fi and Wireless Solutions	✓	✓	✓	✓	✓	
Mobile Hotspots & Wi-Fi Bus Solutions	✓	✓	✓	✓	✓	✓
COMMUNICATION						
Voice Over IP Services	✓		✓		✓	
Unified Communications Solutions	✓		✓		✓	
SECURITY						
Security Solutions	✓		✓		✓	
Cloud Solutions	✓		✓		✓	
Endpoint Protection	✓		✓		✓	
STUDENT ENGAGEMENT						
Engagement Analytics	✓	✓	✓	✓	✓	
Zoom	✓	✓	✓	✓	✓	

** The ECF can also be used to fund Private LTE networks in areas without sufficient commercially available Internet service, or for the purchase of the end user equipment required to connect to private LTE networks.*

PARTNERING FOR SUCCESS

ENA has been helping school districts across the nation shape and achieve their technology missions and goals for over 25 years, achieving an industry-leading NPS score of 90. As an experienced technology partner, we understand the unique needs and challenges education communities face, and we go above and beyond to provide them with the services and customer support they require to serve their students and staff. To learn more about our ESSER-eligible connectivity, security, and communications solutions, or to request a meeting with one of our experts, please visit www.ena.com/funding-eligibility/.

ENA delivers transformative connectivity, communication, cloud, security, and data analytics solutions supported by exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.