OFFICE OF
Educational Technology

Building Technology Infrastructure for Learning

JUNE 2017

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

Building Technology Infrastructure for Learning Guide
U.S. Department of Education

June 2017
Version 2.0

Examples Are Not Endorsements
This document contains examples and resource materials that are provided for the user's convenience. The inclusion of any material is not intended to reflect its importance; nor is it intended to endorse any views expressed, or products or services offered. These materials may contain the views and recommendations of various subject matter experts as well as hypertext links; contact addresses and websites to information created and maintained by other public and private organizations. The opinions expressed in any of these materials do not necessarily reflect the positions or policies of the U.S. Department of Education. The U.S. Department of Education does not control or guarantee the accuracy, relevance, timeliness, or completeness of any information from other sources that is included in these materials.

Licensing and Availability

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

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

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

Contents

Acknowledgments

Project Team

The 2017 update of the Building Technology Infrastructure for Learning Guide was published by the U.S. Department of Education, Office of Educational Technology (OET).

Susan Bearden served as the principal lead in updating the guide. Within OET **Christine Stokes-Beverley**, **James Collins**, **Peter Hutchinson**, **Fatima Jibril**, **Sharon Leu**, **Rebecca Mathews**, **Kristina Peters**, **Jacqueline Pugh**, **Sara Trettin**, **Angela Vann**, and **Casandra Woodall** provided technical assistance.

Additional 2017 Building Technology Infrastructure for Learning updates were provided by the following K-!2 Chief Technology Officers and other subject matter experts: **Jamie Britto** (Collegiate School), **Andrew Chlup** (Anchorage School District), **Beulah Daniel** (District of Columbia Public Schools), **Jeff Dayton** (Madeira School), **Cameron Dixon** (U.S. Department of Homeland Security), **Diane Doersch** (Green Bay Area Public Schools), **Jack Johnson** (Anchorage School District), **Mark Johnson** (MCNC), **Sara Kloek** (U.S. Department of Education), **Karen S. Magara** (Salamanca City Central School District), **Rick Miller**, (Santa Ana USD, Ret.), **Nell Hurley** (Education Superhighway), **Davina Pruitt-Mentle** (National Institute of Standards and Technology), **Jim Pulliam** (Orange County Public Schools), **Tom Rolfes** (Network Nebraska), **John Schauble** (Federal Communications Commission), **Susannah Spellman** (Internet2), **Kathleen Styles** (U.S. Department of Education), **Valerie Truesdale** (Charlotte-Mecklenburg Schools).

In addition, the following individuals provided additional assistance and support of the 2017 Building Technology Infrastructure for Learning: **Dennis Bega** (U.S. Department of Education), **Matt de Ferranti** (National Indian Education Association), **Bryan Ford** (NTCA-The Rural Broadband Association), **John Forkenbrock**, (Organizations Concerned About Rural Education) **Karen Hanson** (National Telecommunications and Information Association), **Lisa Hone** (Federal Communications Commission), **Frank Huston** (Terracom Direct), **Keith Kreuger** (CoSN, The Consortium for School Networking), **Noelle Ellerson Ng** (AASA, the School Superintendents Association), **Robert Olsen** (Compass Cybersecurity), **Allen Pratt** (National Rural Education Association), **Richard Quinones** (iBoss), **Jean Rice** (National Telecommunications and Information Association), **Emy Tseng** (National Telecommunications and Information Association), **Danae Wilson** (Nez Perce Tribe), **John Windhausen** (Schools, Health, and Libraries Broadband Coalition), **Kelly Wismer** (NTCA-The Rural Broadband Association).

The 2014 Building Technology Infrastructure for Learning guide was developed under the guidance of **Bernadette Adams**, **Zac Chase**, **Richard Culatta**, and **Joseph South** of the U.S. Department of Education, Office of Educational Technology.

Marianne Bakia of SRI International led the 2014 guide development and drafting. Other contributing authors were **Marie Bienkowski**, **Sarah Nixon Gerard**, **Jim Klo**, and **Gloria I. Miller**. **Jennifer Knudsen**, **Rob Muller**, and **Phil Vahey**, also of SRI International, provided advice and insightful feedback on drafts. **Eryn Heying** provided research assistance, and **Brenda Waller** provided administrative assistance. **Kate Borelli** produced graphics and layout.

Susan Thomas, independent consultant, supported the development team with substantive editing, writing, and advice.

Graphics were developed by SRI in Washington, D.C. Appendix A Graphics were provided by Internet2.

Interviews

The authors of the guide thank the experts interviewed for this guide: **Kristen Atkins** (Qualcomm), **Denise Atkinson-Shorey** (e-Luminosity), **Wayne Beasley** (Craven County Schools, North Carolina), **Cathy Benham** (CSM Consulting), **Kevin Carman** (Education Channel Marketing, AT&T), **Fred Dyste** (Digital West Networks), **Kim Friends** (CSM Consulting), **LeRoy Hardy, Jr.** (Dicoer Education Technology Management), **Lisa Hone** (Federal Communications Commission), **Greg Klein** (Rogers Family Foundation), **Keith Krueger** (Consortium for School Networking), **Jen Leasure** (The Quilt), **Greg Mathison** (CISCO), **Evan Marwell** (Education Superhighway), **Carroll McGillin** (CISCO), **Sujeet Rao** (U.S. Department of Education), **Tom Rolfes** (Network Nebraska), **Teri Sanders** (Imperial County Office of Education, California), **Susan Silveira** (Qualcomm), **Michael Steffen** (Federal Communications Commission), **Kathleen Styles** (U.S. Department of Education), **Mary Veres** (Sunnyside Unified School District, California), **Matt Wallaert** (Microsoft/Bing), and **Luis Wong** (Imperial County Office of Education, California).

Technical Working Group

In addition, a Technical Working Group of K-12 chief technology officers reviewed drafts of the guide and provided invaluable feedback, writing, and examples from their experiences. Many thanks to **Steve Clemons** and **Greg Ottinger** (San Diego County Office of Education, California), **Michael Evans** (Forsyth County Schools, Georgia), **Patrick Larkin** (Burlington Public Schools, Massachusetts), **Maribeth Luftglass** (Fairfax County Public Schools, Virginia), **Jeff Mao** (Maine Department of Education), **Patrick Martin** (U.S. Department of Defense Education Activity), **Steve Midgley** (U.S. Department of Education), **Fran Newberg** (Philadelphia School District, Pennsylvania), **Adam Seldow** (Chesterfield School District, Virginia), **Scott Smith** (Mooresville Graded School District, North Carolina), and **Bob Swiggum** (Georgia Department of Education).

Introduction: The Promise of Ubiquitous Connected Learning

Technology can be a powerful tool for transforming learning. It can help affirm and advance relationships between educators and students, reinvent our approaches to learning and collaboration, shrink long-standing equity and accessibility gaps, and adapt learning experiences to meet the needs of all learners.

— *2017 National Education Technology Plan*

The U.S. Department of Education's National Educational Technology Plan (NETP) presents a model of learning powered by technology to help the nation's schools provide all students with engaging and powerful learning content, resources, and experiences.

Technology can give students 24/7 access to information and resources that enable them to find, curate, and create content and connect with people all over the world to share ideas, collaborate, and learn new things. For the vision established by the NETP to be fully realized, access to online tools and resources needs to be reliable and ubiquitous inside as well as outside school. To provide students with the education they need to thrive in a globally connected world, we must find ways to design, fund, acquire, and maintain the infrastructure that will make connectivity a reality for every teacher and student in every learning environment.

This guide provides practical, actionable information intended to help both technical personnel and educational leaders navigate the many decisions required to deliver broadband connectivity to students. It presents a variety of options for school and district leaders to consider when making technology infrastructure decisions, recognizing that circumstances and context vary greatly from district to district.

About The 2017 Update

In the nearly three years since this guide was originally published, the school broadband connectivity landscape has seen many changes. In 2014, 25 percent of districts reported that *not a single school in their district could meet the Federal Communications Commission's (FCC) short-term connectivity goal of 100 Megabits per second per 1,000 students*.[1] By comparison, in 2016, 80 percent of districts reported that at least three-quarters of their schools had achieved this immediate connectivity goal.[2]

The 2014 modernization of the Schools and Libraries Universal Service Support Program, also known as the E-Rate program, an FCC program that provides technology infrastructure funding for eligible schools and libraries, brought broadband connectivity and the funding for wireless infrastructure upgrades to thousands of schools and classrooms across the nation. These changes have made it possible for teachers and students to explore new learning models, new digital learning environments, and new approaches to working, learning, and sharing.[3]

Despite this tremendous progress, there are still schools and districts, particularly in rural areas, that do not yet meet the FCC's short-term school connectivity goal of 100 Mbps per 1000 students. School systems identify recurring bandwidth expenses as the biggest barrier to robust connectivity, with 29 percent of rural districts reporting that geography is also a significant barrier.[4] In addition, 54 percent of rural districts report that they have only one Internet Service Provider (ISP) to choose from, meaning they often pay much higher bandwidth prices than urban/suburban schools due to the lack of competition.[5] Finally, high up-front construction costs for fiber mean that schools in the most remote areas are often limited to older networking technologies such as Digital Subscriber Line (DSL) or copper lines, or rely on costly satellite Internet technologies that are subject to data limits and weather interference.

This update serves as a roadmap for schools and districts looking to modernize the technology infrastructure needed for digital learning, providing both concrete advice and aspirational recommendations. No matter what stage districts or schools are at on the journey to digital learning, this guide will help them move forward.

The Need for Speed

Concerted efforts at the federal, state, and local levels over the last decade have brought Internet connectivity to nearly all of the nation's schools and libraries. Despite these advances, connectivity in some areas remains inconsistent and inadequate to handle the demands of modern digital learning environments. Bandwidth needs are not static and continue to grow with advances in technology. According to Education Superhighway, K-12 bandwidth demand has been growing at a rate of 50 percent each year.[6] Schools require reliable, scalable connectivity to provide students access to the digital tools necessary for a world-class education. To meet these needs, schools must have a robust technical infrastructure that extends high-speed wireless connectivity to every classroom and instructional space.

Lack of high-speed broadband is disproportionately common in rural areas, tribal lands, and other under-resourced communities. Without adequate access, students in these areas miss the benefits of many educational technologies entirely. In addition, they miss the opportunity to develop the critically important digital literacy skills needed for success in today's workforce. Gaps in access to broadband tools and content exacerbate other, preexisting inequities in under-connected schools and unconnected homes. This "digital divide" has educational, social and economic implications for entire communities, limiting access to educational and career opportunities.[7]

For school staff, inadequate broadband access negatively impacts employee productivity and efficiency. Educators without high-speed Internet cannot fully participate in many high-quality professional development opportunities. Examples include joining streaming global professional conferences, sharing video of their practice with online peer-coaching groups, and leveraging digital technologies to work more closely with students. Often, these teachers must work from

home after hours, where they have access to a faster Internet connection. In addition, staff may have difficulty accessing cloud-based resources used to support school operations such as student information systems or online grade books.

BROADBAND

Broadband refers to high-speed Internet access that is always on and significantly faster than traditional dial-up access. In January 2015, the FCC upgraded their definition of broadband speeds to 25 Mbps for downloading content and 3 Mbps for uploading content.[8] Types of broadband include digital subscriber line (DSL), cable modem, fiber, wireless, satellite, or broadband over power lines (BPL).[9]

Recognizing the need for student and teacher access to high-speed Internet, in 2014, the FCC modernized the E-Rate program to better support broadband access. As part of the modernization, the FCC adopted a short term goal of connecting all schools and libraries to the Internet at speeds of no less than 100 Mbps per 1000 students and a target speed of 1 gigabit per second (Gbps) by 2018.[10] Since 2013, the effort to connect America's students to 21st century learning has delivered high-speed broadband to 88 percent of public school districts.[11] However, 11.6 million students in more than 19,000 schools still lack the minimum connectivity necessary for digital learning.[12]

BANDWIDTH TERMS

Bandwidth is the amount of data that passes through a network as measured in bits per second (bps).

Kbps is short for kilobits per second. A kilobit is a data transfer rate of 1,000 bits per second.

Mbps is short for megabits per second. A megabit is a data transfer rate of 1,000,000 bits per second. The State Educational Technology Directors Association (SETDA) recommends that by the 2017-2018 school year school districts should have, on average, 1 Mbps per user (students, faculty, and staff).[13]

Gbps is short for gigabits per second. A gigabit is a data transfer rate of 1,000,000,000 bits per second. SETDA recommends that by the 2021-22 school year, school districts should have, on average, 3 Mbps per user (students, faculty, and staff).[14]

Technology infrastructure is just one element of educational transformation. Equally important is the investment in high-quality professional learning and instructional methodology so teachers enter classrooms ready to use the new tools to support blended and personalized learning for all students. Technology use should be guided by clear goals and effective planning, which requires that stakeholders in the system act together and plan beyond technology alone. Therefore, this guide also provides considerations for digital learning resources and staff professional development, and addresses other implementation issues such as device selection, responsible use policies, privacy, and security associated with creating effective connected schools.

THE NATIONAL EDUCATIONAL TECHNOLOGY PLAN

The National Education Technology Plan (NETP) articulates a vision of equity, active use, and collaborative leadership to make everywhere, all the-time learning possible. For more information about crafting a comprehensive district educational technology plan, consult other resources, starting with the NETP. This infrastructure guide focuses on the steps and decisions districts should consider in implementing the technological infrastructure to support a comprehensive educational technology plan. This guide does not address the other key steps in such a plan, for example, determining how students will use technology to advance learning goals, how to provide teachers with the training necessary to use these tools, and what content and instructional methods to use.

1. Getting Started

IN THIS SECTION

- Planning and leadership demands associated with technical upgrades
- Key questions for assessing conditions in schools and districts
- Setting technical goals for the future

Technology-supported learning enables students to create digital media, collaborate with experts and learners across the world, and employ tools to access deeper, more personalized learning. Teachers, parents, and students are looking to schools to provide high quality, sustainable learning tools and reliable connectivity.

PILOTING TECHNOLOGY ROLLOUTS

Examples abound of poorly planned, large-scale technology rollouts that failed to positively impact student learning. Inadequate network infrastructure, insufficient teacher professional development, and lack of user buy-in are just a few of the many factors that can cause a rollout to fail. Instead of implementing new technologies on a wide scale, consider starting with small pilots and iterative, phased implementation approaches. This will allow technology staff to address unanticipated glitches and gather critical user feedback before expansion. Make sure the necessary network infrastructure is in place before deploying devices and incorporate administrator, teacher, student and parent input before scaling the initiative.

While getting connected devices in the hands of students and teachers is important, it takes much more to shift teaching practices within classrooms, schools, and districts. For systemic changes to occur, school and district leaders need to create a shared vision for how technology can best meet the needs of all learners and develop a plan that translates that vision into action.[15] This vision will provide the compass by which institutions can steer the process outlined in this guide. A solid network infrastructure lays the foundation for successful education technology implementations, but is one of only the many factors necessary. A proper infrastructure, defined in the broadest terms, also provides for the capacity of buildings, tools, policy, systems, and people.[16]

This section explores some important elements of the process.

LOOK TO THOSE WHO HAVE COME BEFORE

Consider the efforts of schools and districts that have previously launched successful digital learning initiatives to prevent missteps and avoid wasting time and funds. More experienced schools and districts such as those referenced in this guide can share best practices and lessons learned.

Guidance is available from state and national agencies and nonprofit organizations such as:

- Alliance for Excellent Education
- CoSN
- Digital Promise
- Education Superhighway
- ISTE
- National Clearinghouse for Educational Facilities
- Project RED
- SETDA

School leaders should consult their state department of education for further guidance. For example, the New Jersey Department of Education has a Facilities Guide for Technology available online. Many districts post technology plans online that can serve as examples, like New York City Public Schools and Plymouth Public Schools in Plymouth, CT.

Successful digital learning transitions require strong school and district leadership at the helm. Superintendents and other senior school leaders should assemble high-level teams to develop a unified vision for how technology can support educational goals. These teams should include senior leadership in technology operations and curriculum, the chief financial officer, and other community stakeholders including parents, teachers, and students.

After identifying a strong planning team, the next step is to assess the capacity of current network infrastructure and devices, gauge current levels of usage, and estimate the demands needed in the future. This assessment will help determine which parts of the current infrastructure need to be replaced, upgraded, or supplemented.

The following seven questions can guide an evaluation of district Internet needs and capacity.

HIRE THE BEST

Schools and districts looking to hire a district technology lead/chief technology officer (CTO) or chief information officer (CIO) may wish to consult the Consortium for School Networking (CoSN) framework of essential skills for K-!2 CTO's: http://www.cosn.org/Framework.

1. What is the vision for learning that technology will be supporting?

Bandwidth requirements within schools and districts depend on how technology is used to support teaching, learning, and assessment. Although it's easy to be drawn in by flashy promotional materials and discounts, schools and districts should articulate how students will use technology to learn before making decisions about technology. Learning objectives should drive the technology implementation and not the other way around. Once the learning objectives have been identified, success measures can be determined.

Community and stakeholder ownership is key to the success of any major school initiative. Involve stakeholders, such as senior school and district leaders, board members, curriculum directors, school administrators, teachers, students, parents, and other community leaders across all stages of planning and implementation and establish transparent policies and procedures. Communicate these policies to stakeholders and, when possible, remain flexible and responsive to the needs of individual schools.

PUTTING LEARNING FIRST

To address long-standing academic concerns, Revere High School in Revere School District in Massachusetts implemented a school-wide blended learning model. Teachers post lectures, videos, and assignments online for the entire school community to access. Educators have access to virtual tools that facilitate collaboration with school leaders, allowing them to receive more immediate feedback and access online professional development resources. The school's student achievement results have shown growth, particularly compared to peer schools, and Revere received the High School Gold Award from the National Center for Urban School Transformation.[17] A robust investment in supporting teachers and leaders with technology-enabled tools can transform instruction and generate dramatic improvement in student outcomes.

During conversations with students and instructional leaders, senior leadership should ask how they envision technology being used both inside and outside the classroom. If part of the instructional plan is for students to use devices at home, it is important to have a realistic picture of how many students have reliable home Internet access. Surveying families through an initial home access inventory will reveal what percentage of students have access to broadband Internet at home and guide what needs to be done to bring connectivity to all students. The CoSN Digital Equity Action Toolkit has a sample out-of-school connectivity survey that may serve as a helpful template.

After developing a better understanding of district connectivity, consider convening families and community leaders for discussions of digital equity. New plans for technology use and infrastructure within schools can provide the perfect opportunity to engage the larger community in conversations about what it means to be a connected community. *See Section 4. Getting Devices to Students and Teachers for additional information about ensuring home access.*

2. What digital tools will be needed?

Talk with students, teachers, and school administrators to understand how they currently use learning technologies. Augment these informal conversations by holding listening sessions or organizing standing advisory groups to ensure clear communication channels. Seek guidance from state assessment officials regarding projected testing demands on technology resources.

Consider how high-speed broadband and new devices will enable schools to take advantage of additional digital learning content and resources. Technologies used in audio/video production and videoconferencing require a large amount of bandwidth, especially when used by many students simultaneously. Consider the potential demands of administrative software, security, web hosting, and other applications and plan how to adapt to technology demands down the road. *See Section 4. Getting Devices to Students and Teachers for more information on digital learning resources*.

EVALUATING EDUCATIONAL TECHNOLOGY TOOLS

The Rapid Cycle Evaluation (RCE) Coach is free, web-based platform that supports K-12 school and district leaders in conducting short cycle evaluations of educational technologies already in use or for future use at their schools. Developed by the U.S. Department of Education in partnership with Mathematica Policy Research and SRI, it includes a five-step process for educators to create a research design, including formulating a targeted research question, planning the evaluation, documenting the context, collecting the data and analyzing the results. The goal of the RCE Coach is to increase evidence-based decision making related to the procurement and implementation of educational technologies.

Other resources to support evidence-based decision making about educational technologies include the Lea(R)n Platform, EdSurge Concierge and Product Index, Common Sense Education, and the What Works Clearinghouse.

The Institute of Education Sciences Education Research Grants Program and the Special Education Research Grants Program support evaluations of innovative forms of education technology designed to improve student learning, support teachers, and strengthen schools. The Education Research Grants Program offers 12 topics to choose from and the Special Education Research Grants Program offers 11 topics. While technology-related proposals are appropriate across all of the topics, two are specifically designated for technology. The Education Technology Topic focuses on learning technologies with the goal of improving academic performance in reading, writing, math, and science among K-12 students. The Technology for Special Education Topic focuses on technology tools that are designed to improve outcomes for infants, toddlers, preschool children, and K-12 students from with or at risk for disabilities.

The Institute also offers a grant program for Low-Cost Short Duration Evaluation of Education Interventions. Through this program, developers and researchers can submit applications for rigorous evaluations of education interventions (broadly defined as practices, programs, and policies) that state or local education agencies expect to produce meaningful improvements in student education outcomes within a short period (for example, within a single semester or academic year).

3. What kind of professional learning will teachers and administrators need?

Although districts can distribute devices and links to learning resources, administrators and teachers who do not understand how these tools support their work may not use them. Solving this problem will take time and training. Because educators differ in technology expertise and pedagogical knowledge, professional learning should be designed to meet the needs of teachers at all levels, from the most traditional teachers to the earliest adopters of new technologies. This may mean providing administrators and teachers with differentiated instruction that combines in-school and online professional learning communities. Consider ISTE's technology standards for administrators, teachers, and instructional coaches when designing professional learning expectations.

Administrators, teachers and support staff will require a significant amount of professional learning opportunities throughout the year to ensure that the transition to digital learning is successful and lasting. While not the focus of this guide, ongoing, fully funded professional learning regarding research-supported practices for technology in education is extremely important to any successful academic effort.

PROFESSIONAL LEARNING PATHWAYS

The San Diego County Office of Education's Professional Learning Center (PLC) provides county educators opportunities to learn more about instructional technologies through face-to-face workshops, blended courses, online courses, professional networks, strategic technology planning opportunities, and outreach opportunities. Many of the blended and online professional development courses have university credit options and/or national certifications provided. Consider offering multiple professional development options that enable teachers to personalize their professional learning.

4. How much bandwidth will be needed?

Specific data about bandwidth usage should be available from an organization's ISP. Schools that manage their own network should have monitoring tools that provide a comprehensive and accurate bandwidth usage assessment. Schools and districts should consider setting aspirational connectivity target bandwidth recommendations, such as the recommendations from SETDA's Broadband Imperative II, based on the number of users:[18]

INTERNET SERVICE PROVIDER RECOMMENDATIONS		
School Year	2017-18 School Year Target	2020-21 School Year Target
Small School District (fewer than 1,000 students)	At least 1.5 Mbps per user (Minimum 100 Mbps for district)	At least 4.3 Mbps per user (Minimum 300 Mbps for district)
Medium School District (3,000 students)	At least 1.0 Gbps per 1000 users	At least 3.0 Gbps per 1,000 users
Large School District (more than 10,000 students)	At least 0.7 Gbps per 1,000 users	At least 2.0 Gbps per 1,000 users
WIDE AREA NETWORK (WAN) RECOMMENDATIONS		
Connections to each school to link to the Internet via a district aggregation point and for in-house administrative functions	At least 10 Gbps/1,000 users	At least 10 Gbps/1,000 users
User: students, teachers, administrators, staff, and guests Source: The Broadband Imperative II, 2016 by SETDA, used under CC-BY 4.0		

Schools and districts should take the bandwidth demands of online testing into account when developing networks. Those using the PARCC, Smarter Balanced, or other online assessments should check the respective websites of these organizations for minimum requirements and capacity planning tools. In addition, consider other network applications that may impact available bandwidth, such as security systems.

Web-based bandwidth speed tools such as SchoolSpeedTest.org can provide a snapshot of a network's usable speed at a given moment in time. Speed tests can be helpful in determining available bandwidth, but cannot pinpoint the exact source of internal network bottlenecks. Actual network performance will vary based on a variety of factors, including the number and type of simultaneous users and the type of applications being used. Network monitoring services, which provide end-to-end monitoring of a network over time, can provide more granular data. If choosing an independent vendor to manage the network, consider requesting network monitoring as part of the agreed-upon services. Schools that maintain their own network should be able to do network monitoring in house.

5. What will be the needs of the in-school network?

Some buildings, especially older ones, may provide additional challenges for schools wishing to build out or upgrade their network. A network assessment, conducted by school technology support teams or a certified consultant, is the first step. The assessment will identify mechanical, electrical, and environmental conditions that need to be addressed. Examples include the location and condition of existing network cabling and hardware, the number and location of existing wireless access points, and physical building attributes that interfere with wireless signals. Beyond the network assessment, consider additional physical infrastructure questions

such as the number of electrical outlets available in classrooms to charge mobile devices. *See Section 3. Getting High-Speed Internet Throughout Schools—Planning a Network, for more information on these and other network infrastructure questions*.

6. How many and what type of devices are needed?

Once a clear vision for the role of technology in learning and teaching has been established, determine how many wired and wireless devices the network will need to support. First, determine the type of devices that are needed for educational use, taking into account student accessibility needs. Second, consider the number of devices that students and teachers can connect to the school network. Be sure to differentiate between devices owned by the school district and those that are personally owned by students and staff. Wireless networks should be designed to provide adequate coverage, which is the breadth of area in which wireless access is available, and density, which is the number of devices that can connect to and use the network in a confined place such as a classroom. *See Section 3. Getting High-Speed Internet Throughout Schools for additional information on estimating bandwidth needs.*

Take an inventory of the types of devices currently owned and in use by the school—desktops, laptops, tablets, and/or smartphones—and when they will reach end of life. The refresh cycle for devices will vary, but is generally between 3-5 years. Older devices with slower processors and/or less powerful Wi-Fi antennas might not be able to benefit from faster wireless speeds and will need to be upgraded or replaced. Be sure to plan for device replacement during the budgeting process. *See Section 4. Getting Devices to Students and Teachers—Structuring Device Purchases, for additional information on purchasing devices*.

REMEMBER PERSONAL DEVICES

Under a BYOD (Bring Your Own Device) policy, students may be permitted to bring their own laptop, tablet, smartphone, or other Internet-enabled device to school. When planning for bandwidth needs, don't forget to account for these personal devices, keeping in mind that students may bring multiple devices to school. For most schools, the way that students and staff access the school Wi-Fi network with personal devices should differ from how they access the network with school-issued devices. For more information on network planning, see *Section 3. Getting High-Speed Internet Throughout Schools*. *For more about BYOD policies, see Section 4. Getting Devices to Students and Teachers*.

7. What resources are available to fund the transition?

One of the most important resources available for the transition to sustainable broadband connectivity in schools is the E-Rate program. The FCC's E-Rate program provides discounts between 20 percent to 90 percent to help eligible schools and libraries pay for Internet connectivity and maintain internal network connections, including Wi-Fi networks. The highest discounts are provided to high-poverty and rural schools and libraries. For additional information about E-Rate, see the E-Rate Funding for Internet Connectivity section.

In addition to E-Rate, some federal education grants may be applied to support the transition to digital learning. In October 2016, the U.S. Department of Education released Non-Regulatory Guidance for the Student Support and Academic Enrichment (SSAE) Grants. The Department also released a Dear Colleague Letter which outlines how funds under Titles I through IV of the Elementary and Secondary Education Act (ESEA), as amended by the Every Student Succeeds Act (ESSA), and the Individuals with Disabilities Education Act (IDEA), may support the use of technology to improve instruction and student outcomes, as long as those solutions align with the purpose and constraints of the Title. At the state level, examples of innovative funding models can be found in State Digital Learning Exemplars from SETDA and the Friday Institute.[19] There are also innovative cost-saving models worth considering. For example, some schools have partnered with other area educational institutions or even their town or city to pool bandwidth needs and create local or municipal networks that save all parties money.

Each section of this Guide points to funding resources and suggestions specific to its topic. For a comprehensive list of connectivity funding resources please see https://tech.ed.gov/funding/.

The next two sections discuss considerations in upgrading Internet connections to the school and within a school, respectively.

2. Getting High-Speed Internet to Schools

IN THIS SECTION

- Understanding types of available connectivity
- Four paths for connecting districts and schools
- Cost drivers and funding sources to consider
- Special considerations for rural areas

This section provides an overview of the technical details associated with getting broadband Internet to schools. It first reviews the wired and wireless types of connectivity and then outlines how those connectivity types are most commonly used to create high-speed pathways for schools.

TELECOMMUNICATION NETWORK TERMS

Backbone describes the major network connections across the country. Think of them as the major highways of the Internet

Middle mile Refers to the part of a telecommunications network that connects the Internet backbone and regional Internet Service Provider (ISP) or district.

Last mile refers to the connection between the regional ISP and individual school buildings.

Types of Internet Connections

Wired Connections

Wired technologies are faster, less prone to interference, and more reliable than wireless connections. The most common wired technologies are fiber-optic cable (known as fiber) and Data Over Cable Service (known as cable or DOCSIS). The easiest way to take advantage of either of these options is to use wires that have already been installed. Cable wiring is likely to be the most prevalent, but fiber provides faster and more reliable connections and is often less expensive in the long run. Installing fiber requires specialized training and equipment and often requires underground trenching or stringing the fiber from telephone poles to connect the ISP to the school or district. Fiber installation costs are substantially lower when the trench has already been dug or when fiber has been strung aerially for the majority of distance and trenched from the poles to schools.[20] Many states and municipalities are instituting "Dig Once"

policies, which lower fiber installation costs by providing access to state- or city-owned rights-of-way and mandate the installation of fiber conduit during road construction projects.

Consult with ISPs and utility and municipal institutions to understand the existing and potential wired Internet access options in a local area. When comparing costs, consider the total cost of ownership (see below), and regional availability. The Education Superhighway *Compare and Connect* tool enables schools and districts to compare their bandwidth costs with those of other districts.

FIBER-OPTIC DEFINITIONS

Dark fiber is fiber optic cable that has already been laid, generally underground, but does not have the networking equipment on each end to connect to the Internet.

Indefeasible right of use (IRU) is a contract to use someone's dark fiber for a long period at a low cost. A district that acquires fiber through an IRU is responsible for providing the equipment to connect (or light) the fiber.

Leased fiber is a contract between an ISP and a district whereby the ISP agrees to deliver Internet services using fiber owned by a public telephone network or other provider. The connection fee is a fixed monthly rate determined by the distance and speed provided. Leased fiber can either be dark (as in an IRU) or include all the required network equipment (lit fiber).

INTERNET OVER FIBER

Fiber consists of a thin cylinder of glass encased in a protective cover that uses light rather than electrical pulses to transmit data. Each strand of the cable can pass a signal in only one direction, so fiber-optic cable must have at least two strands: one for sending data and one for receiving data. Fiber-optic cables are not subject to electrical interference, which greatly increases the transmission distance. Most schools do not own their own fiber (similar to telephone or electric lines) although the 2014 E-Rate modernization order does provide E-Rate funding for schools wishing to "self-provision" fiber when it is the more cost-effective option. This is sometimes the case in rural areas. The two most frequently used options for acquiring fiber Internet access are leasing or obtaining a right of use contract.[21,22]

An indefeasible right of use contract (IRU) generally provides complete use of a fiber line without any limitations for an extended period of time. IRUs are often negotiated on terms similar to mortgages (e.g., 15–30 years) with a single payment up front. IRUs typically come from utility companies, telecommunications companies, or railroads that maintain and service dark fiber. Fiber obtained through an IRU is dark fiber, since it does not come with any of the network equipment required to activate it, and substantial up-front costs to light the fiber must be factored in. However, IRUs can result in significantly reduced long-term costs relative to leasing.

With leased fiber, the owner retains overall control over the fiber and provides the school or district with the ability to use a certain amount of capacity based on the lease agreement. Similar to an IRU, unused dark fiber can be leased, requiring the district to provide the network equipment to activate the fiber. However, the technical challenges associated with setting up and managing a fiber optic network can be considerable.[23]

There are also options to lease lit fiber at a higher cost that already includes all the required network equipment. Leases are usually shorter contracts (e.g., 1–5 years) with monthly payments to the service provider. Districts can choose to use less than the full capacity of the fiber up front and pay for additional capacity later if it becomes necessary. Although more expensive, lit fiber costs may be more predictable.

Either through an IRU or a lease, dark fiber can provide almost limitless future capacity at a marginal cost because the expense in increasing bandwidth generally comes from the network equipment that is connected to the fiber, not the fiber itself.

Self-provisioned fiber networks are run and maintained by a school or district. Although self-provisioning gives schools the most flexibility in operating and maintaining their networks, it has the highest upfront capital costs. Most schools and districts pay a contractor for fiber maintenance.[24] The 2014 E-Rate modernization allows for schools and districts to use E-Rate funds for self-provisioning if they can demonstrate it is the most cost-effective solution.

CONNECTING VIA FIBER THROUGH CREATIVE APPROACHES

In 2011, Chesterfield County Public Schools in Virginia had a network that was slow and unreliable, especially for remotely located schools, which prevented many teachers from using digital media with their students. As part of an ambitious district strategic plan to support blended learning, the district technology team designed and implemented a complete leased fiber network, which required the vendor to provide equitable bandwidth to all schools and administrative buildings. The upgraded fiber network enabled Chesterfield in recent years to deploy 38,000 Chromebooks as part of a 1:1 program in grades 6-12 and handle the increasing bandwidth demands of technology-infused teaching and learning. In addition to leveraging E-Rate funding, the district helped recoup the expenses associated with the network upgrade by reducing print textbook purchases and moving to Open Educational Resources (OER). Chesterfield has been recognized by the U.S. Department of Education as a #GoOpen Ambassador District.

Butte School District in Montana initiated a public-private partnership in 2013 with a fiber provider and the Montana Economic Revitalization and Development Institute to build a new network connecting the district office with all district schools.[25, 26] The district has an IRU with the telecommunications provider that built the network. Now all nine Butte schools have access to dual 1 Gbps fiber connections. Two separate physical fiber connections to each site provide greater speeds and redundancy. The new connections are fast enough to enable video conferencing between classrooms, allow teachers to complete online professional development, and give every student simultaneous high-speed Internet access. The upgraded connections also made it possible to centralize district services and will make future bandwidth increases much more cost effective.

INTERNET OVER CABLE

Internet service provided over cable has the benefit of using the more prevalent existing cable TV infrastructure, which can reduce the initial cost of installation. However, schools and districts may require more bandwidth than existing cable infrastructure can provide. In some areas, where schools and districts do not have access to fiber, cable Internet connectivity may be the fastest choice. Schools and districts that have fiber connections may also choose to use a cable modem as a backup Internet connection.

Check with providers to get a clear understanding of current circuit capacity and the potential for bandwidth expansion. Make sure whatever bandwidth level negotiated is provided as a guaranteed minimum, and not just an "average" or "best-efforts" level. Schools and districts may wish to consider a multi-year lease with the ability to renegotiate bandwidth and price structure annually.

CHECK TOTAL COST OF OWNERSHIP

When comparing prices of network connections, make sure to compare the price per megabyte, not just up-front costs. To calculate price per megabyte, add all capital expenses and recurring costs and divide by the number of megabytes received. For example, a 1GB connection may cost $1,000 per month, or $1 per megabyte. A 10GB connection may cost $5000 per month—a substantially higher monthly bill but resulting in a cost of only $0.50 per megabyte. Keep in mind, however, that not every school needs a 10GB connection. If a school is only using 1GB but is paying for a 10GB connection, it would be overbuying for its needs.

It can be helpful to use a comparison tool when calculating network design costs. The Analysis of Costs to Upgrade and Maintain Robust Local Area Networks for All K-12 Schools by CoSN and Education Superhighway may serve as a helpful point of reference. In addition, CoSN's Smart Education Networks By Design (SEND) initiative provides a robust range of tools and resources for designing education networks.

Wireless Broadband

In some areas, such as rural regions, neither fiber nor cable service is available. In these situations, wireless solutions may be the best option. Wireless broadband connects a building to the Internet using a radio link between the customer's location and the service provider's facility. Wireless broadband can be fixed or mobile.

FIXED WIRELESS

Fixed wireless options often require a clear line of sight between a tower and the school building (or directly between buildings). These technologies use longer-range directional equipment to provide broadband service in remote or sparsely populated areas where landline service would be costly to provide.[27] Fixed wireless may not work in areas with variable physical terrain or vegetation that prevents a clear line of sight and is not as reliable as a wired Internet connection. In addition, per-megabyte costs are higher than wired connections.

MOBILE BROADBAND

Mobile data services, like those that provide the data service on smartphones, may be available under limited circumstances where schools may have rights to a wireless spectrum based on existing educational spectrum licenses from the FCC. The FCC historically issued these licenses to educational agencies around the country under the Educational Broadband Service Spectrum program. While the FCC is not currently granting any new licenses, the Commission is working on a possible new mechanism for education organizations to apply for this type of spectrum where it is available. Mobile wireless users will experience a small amount of latency, or delays in the processing of network data.

SATELLITE INTERNET

Satellite Internet, which uses satellites orbiting the earth to provide broadband links, is commonly used in remote or sparsely populated areas. Satellite broadband speeds depend on several factors, including line of sight to the orbiting satellite and the weather. When terrain makes other wireless solutions impossible, satellite may be the only feasible option.

Of all the wireless options, satellite is the least reliable, and tends to be the most expensive per megabit per second. It also typically includes monthly usage caps and limited maximum download and upload speeds. Satellite connections are subject to significant latency due to the distance the signal must travel to connect to the satellite, and may not allow for real-time streaming services such as videoconferencing.

Given the various capabilities and restrictions of wireless and satellite technologies, be sure to compare services before deciding on a provider by determining price per megabyte, latency, environmental issues, and any bandwidth usage limits.

Approaches for Connecting Schools

The following section describes possible pathways for schools and districts to connect to the Internet along with the pros and cons.

When possible, schools and districts should consider purchasing redundant secondary Internet connections through different ISPs. This allows for continuous Internet access should any one ISP experiences an outage. Multiple connections can also improve connectivity speeds and provide additional options for the prioritization of Internet traffic.

NETWORK DEFINITIONS

A **Wide Area Network (WAN)** provides the connection *between the* district office and all the schools and sites within a district. A WAN may also connect to other educational institutions (such as universities and libraries) if a school or district is part of a REN.

A **Local Area Network (LAN)** is the network *within a* school or district building through which computers and devices connect to the Internet. LANs, in contrast to WANs, service much smaller geographic areas.

Path 1: Schools Connect Through the District to Research & Education Networks

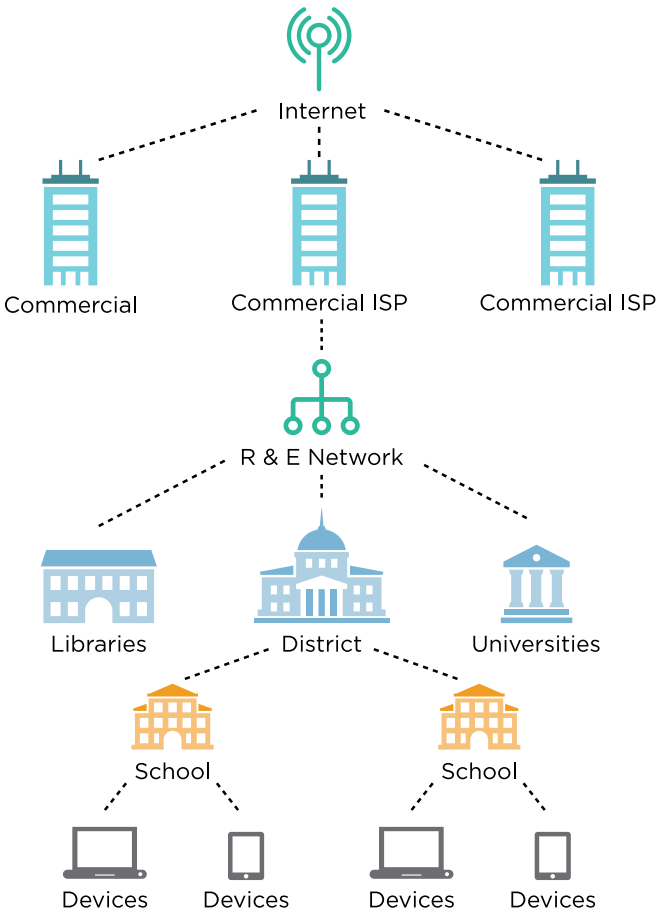
Research and education networks, called R&E networks or RENs, are high-speed, fiber-based broadband networks borne out of the higher education sector and operated by not-for profit organizations or are affiliated with state governments. Approximately 43 state or regional based networks interconnect with Internet2, a national R&E network backbone, and with one another. This creates a private broadband network for education and research purposes, which also interconnect or peer with the commercial Internet. These networks are run by state or regional based consortia, are often associated with higher education institutions, and were originally developed and still operate to meet the unique networking needs of academic and research communities.

RENs vary in their funding and operating models but are engineered to meet the specific demands of their research and education users. RENs are typically funded by a combination of services and member fees and in some states, through public funds. Forty-four states, through partnerships with higher education institutions, the local REN, and other broadband partners (including state or commercial broadband providers), provide K-!2 districts and schools access to the national Internet2 R&E network ecosystem. Depending on the state or location of the school, RENs can provide fiber to the school district or school, work with the district to obtain fiber to the REN network, or work with other broadband providers, including commercial providers, to obtain terrestrial or wireless connectivity to their network.

RENs work with one another and with Internet2 as regional and national consortia partners to save money by pooling bandwidth demand across more users. K-12 districts can leverage the R&E private network and have private network access to any content, resource, or data that housed or hosted at an REN connected institution, which includes universities and colleges, K-12 districts, public libraries, and other national resources, including the Smithsonian, National Archives, and Library of Commerce, without traversing the public Internet. Many cloud-based service providers offering applications to the education sector also interconnect with RENs to allow users access to their online services and applications on the R&E private network. For example, if an online video collection is housed at a university that is part of the REN, the schools can stream or download those materials via the R&E private network instead of using a commodity Internet connection. RENs can provide a high performance and cost-effective solution for normal usage and in many cases, provide a flexible mechanism to manage school bandwidth, i.e., allowing schools to spike Internet bandwidth for short periods, such as for assessments and software updates.

Not all districts are located near a REN connection point. To find out if a REN is located nearby, go to: https://k20.internet2.edu/get-connected. If a REN is available in a region, compare the speed and cost with those of the other paths described below.

Illustrated below is an example of schools connecting through the district to a REN. Note that the REN uses multiple ISP connections to pool bandwidth for members and provide redundancy should an ISP experience an outage.



For additional examples of REN connection paths, see Appendix A.

WHERE THIS PATH MAKES SENSE:

If a school or district is in an area with access to a REN, this may be the most cost-effective method of Internet connection.

Pros: RENs are controlled by their research and education users and are transparent in technical operations and finances. Because RENs are controlled by the users they can optimize costs based on the specific needs of those users. RENs aggregate the demands of all their users for bandwidth and other services e.g. firewalls, security, content filtering to drive lower costs. Some RENs can increase capacity for short periods of time when usage is expected to spike (such as during assessments). Some network traffic (content, data, applications, etc.) that is connected to the national REN ecosystem can leverage the private R&E network, bypassing the commodity Internet. Some content can be housed within the network, improving performance and reducing access costs. RENs can be more reliable because they use multiple Internet service providers.

Cons: E-Rate filings approvals can be delayed which can be financially challenging for small, non-profit RENs. RENs require active engagement of their users to be most effective. RENs may not have facilities at or near the school or district buildings. Upfront REN connection costs, i.e., fiber connections to REN backbone, can be high. Long term cost projections can be difficult because consortia funding model costs may vary with usage rates.

---

i

RESEARCH & EDUCATION NETWORKS IN ACTION

The **North Carolina Research and Education Network** (NCREN), operated by the non-profit organization MCNC, is one of the nation's first statewide education and research networks. It provides broadband communications technology services and support to K-12 school districts, higher education campuses and academic research institutions across North Carolina. MCNC offers NCREN technology tools and services to guarantee equal access to 21st century learning by providing a future-proof technology network that is the foundation for change and innovation in our educational systems. In addition to all public school districts in North Carolina, the NCREN user community now includes: all 17 institutions of the University of North Carolina System and General Administration; 128 North Carolina Charter Schools; 27 of the 36 North Carolina Independent Colleges and Universities; all 58 North Carolina Community Colleges; research institutions and foundations; and, along with the N.C. Office of Information Technology Services and other partners, MCNC provides broadband services for numerous non-profit hospitals and public health agencies through the N.C. Telehealth Network.

Network Nebraska, now in its 10th year of operation, provides 291 K-20 entities with Internet access and high-speed backbone that supports a statewide videoconferencing service and e-learning courses. The self-funded statewide network purchasing consortium operates as a partnership between the Nebraska State CIO's office and the University of Nebraska. Network Nebraska connects through the REN, Great Plains Network, to connect into the national R&E network ecosystem. Network Nebraska aggregates broadband demand across the state's K-12 schools, higher education institutions, and other related community anchors. It also allows for districts to increase their Internet bandwidth during times of peak demand without paying extra costs. For example, one group of 82 school districts and five educational service units in the northeast part of the state cooperatively purchase Internet capacity of 5.25 Gbps per month. Commodity Internet unit costs have decreased 99 percent over the last eight years, and participants are urging the network support staff to research and develop application layer services to further decrease local costs. The consortium provides 100 percent of Nebraska school districts with high-speed Internet connectivity.

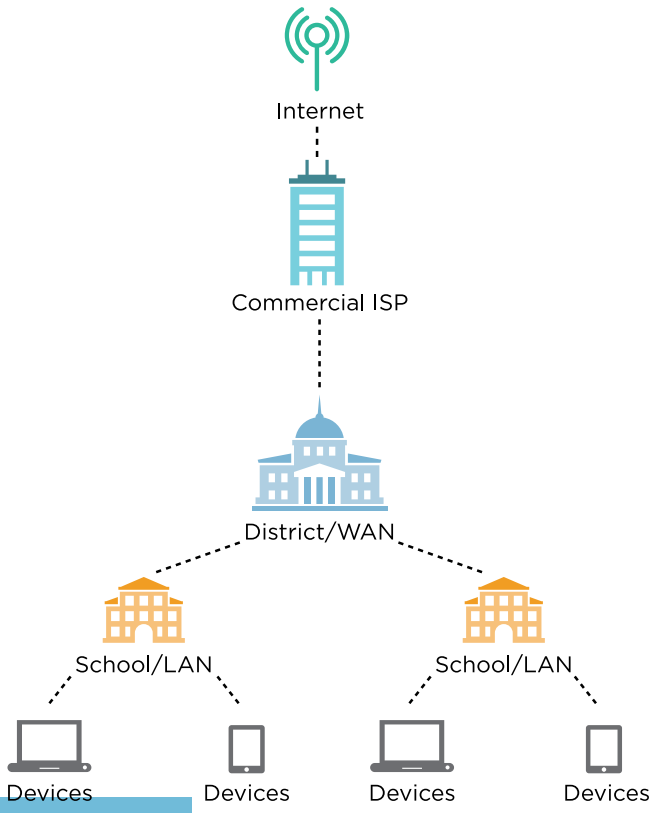
Network Nebraska cooperatively purchases its core routers with the University of Nebraska and leverages state master contracts for its last mile connections (the segments that connect the network backbone to the school). This aggregated demand lowers the cost of connecting schools.

The **Utah Education Network** (UEN) is a statewide, publicly funded partnership between the state's education institutions and local telecommunications providers that connects all of Utah's K-!2 schools, colleges, and libraries to the Internet. UEN also offers its members content filtering, network support, and a learning management system.[28] The foundation of the UEN is a high-capacity fiber backbone. Smaller fiber segments connect the core backbone to WANs, which in turn connect the state's colleges and universities to the Internet. Ninety percent of the state's K-!2 districts connect either directly to that backbone or indirectly through the colleges and universities. Most public high schools and middle schools connect at 100 Mbps with some connecting at speeds up to 1Gbps.[29]

Path 2: Schools Connect Through District to Commercial ISP

On the second path, a district buys bandwidth from a commercial ISP, which provides a high-speed backbone to a centralized district connection. This type of connection is called a middle mile. Schools connect to the Internet through the district wide area network (WAN). Districts can contract with their ISP or another entity to build the infrastructure for their schools' WAN if they do not have the internal capacity to do so. Instead of connecting to a consortium network of other state institutions, districts connect directly to a commercial ISP.

Illustrated below is the path of schools connecting through the district to a commercial ISP.



WHERE THIS PATH MAKES SENSE:

If a local REN does not exist or offer the most cost-effective connectivity, this may be the best option for medium to large districts that can exercise bulk purchasing power.

Pros: Districts can negotiate lower costs by purchasing Internet access on behalf of multiple schools. Temporary capacity increases may be possible when usage is expected to spike, such as during assessments. Pooling capacity allows large schools to share the cost of anticipated usage spikes while smaller schools can take advantage of the lower bandwidth rates. Hardware and services such as firewalls, security, and content filtering can be centralized at the district level, decreasing costs and simplifying management. ISPs may subsidize the cost of building a connection from a district to the ISP network.

Cons: Upfront costs for building a connection from a district to the ISP network can be high. The district building(s) and schools must already be connected via a high-speed wide area network (WAN). To have redundant secondary or tertiary Internet connections, a district must contract with multiple ISPs. This approach lacks the purchasing power and built-in redundancy of a larger REN.

A DISTRICT'S DIRECT PATH TO AN ISP

Forsyth County School District, north of Atlanta, GA serves approximately 46,500 students and is growing at a rate of 1,600 students per year. The district has 37 physical schools and an online school for grades 6–12. For the 2017-18 school year, the district and schools are connected through a redundant fiber network, with a managed 10 GB connection through one ISP and an additional 10GB leased fiber connection that the district manages. In addition to the approximately 3.5 GB connection provided by the state, the district contracts for Internet access from two separate ISPs for an aggregated 19.5 GB of total bandwidth.

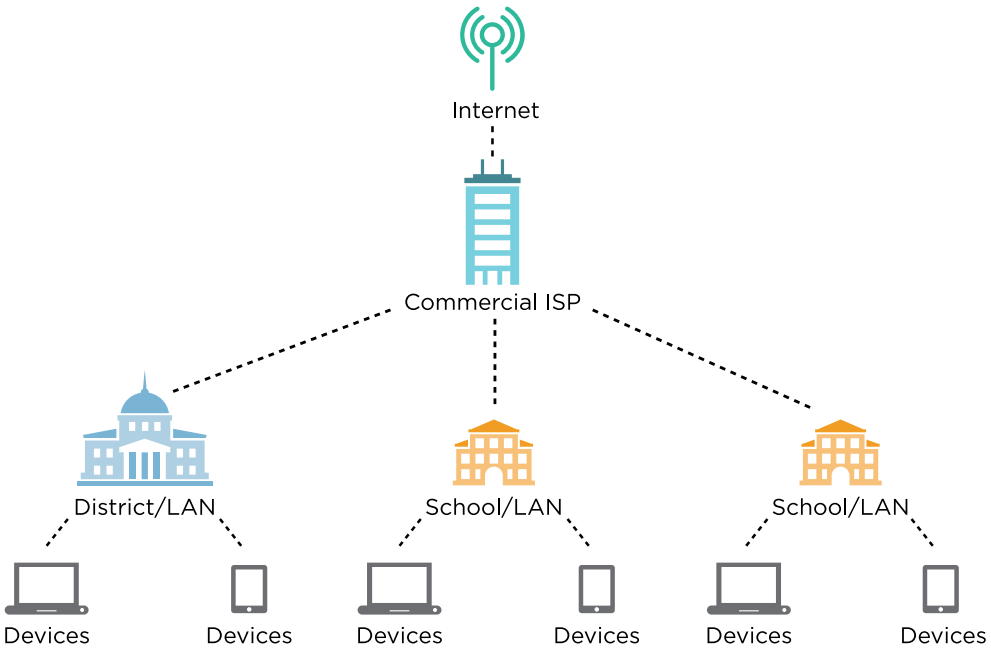
Forsyth's approach has the advantage of multiple ISPs, which allows rerouting of Internet traffic should one ISP experience an outage. Because network management is centralized at the district level, fewer firewall and filter appliances are required. Purchasing bandwidth at the district level enabled the district to negotiate more competitive pricing than purchasing Internet access individually for each school. By incorporating redundant connections from school sites to the data center and maintaining redundant connections to the Internet from the district office, the district mitigates the risk from Internet outages.

Path 3: Schools Connect Directly to Commercial ISP

In the third path, schools connect directly to the ISP for broadband access rather than through a district connection. The ISP manages and maintains the connection right to the school. This can be a more expensive path because opportunities to take advantage of economies of scale are more limited.

The district is still responsible for providing a LAN for distributing connectivity to classrooms and throughout the building as in the other paths, but it does not have to worry about creating a connection to the district or to the ISP.

Illustrated below is the path of schools connecting directly to a commercial ISP.



WHERE THIS PATH MAKES SENSE:

This could be the best path for schools that lack the purchasing power of a medium or large district, do not have the ability to operate a WAN, and do not have access to a REN that offers more cost-effective connectivity. For schools in geographically remote locations, this may be the only option.

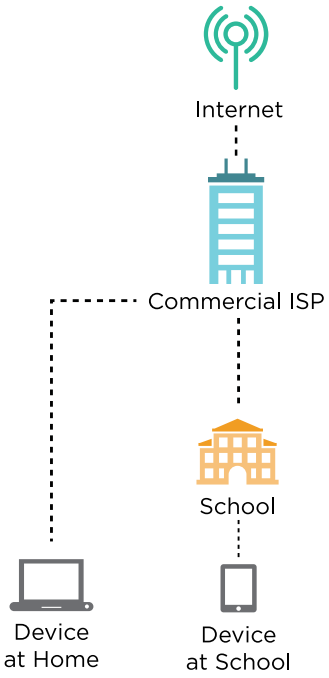
Pros: Districts are not responsible for maintaining a district wide area network because the ISP connects directly to the school. Direct ISP-to-site connections mean that an interruption in connectivity for one school or district building does not result in an interruption for the entire district.

Cons: Upfront costs for building a connection from the schools to the ISP network can be high. The district must contract with multiple ISPs to have redundant Internet access. This path lacks the purchasing power of either RENs or district-purchased Internet access. Without a central district network, this path lacks the capacity to store heavily used content internally.

Path 4: Mobile Devices or Hotspots Connect Directly to Commercial ISP

In the fourth path, a school or district purchases or leases mobile hotspots or cellular broadband-enabled devices from an ISP. This approach can be used anywhere cellular service is available and does not require a connection to a school network. This path is typically used to provide students with equitable connectivity outside school and as a supplement, not a replacement, for in-school connectivity. With this approach, the ISP must implement content filtering and security settings.

The illustration below shows this path, with students connecting an in-school network from on campus and directly to a commercial ISP when off campus.



WHERE THIS PATH MAKES SENSE:

This path could be an option for schools wishing to provide students with home connectivity and/or that face limited school connectivity options.

Pros: Internet connectivity can be provided to students off campus. Schools or districts may not be responsible for maintaining a network if student devices connect directly to the ISP whether on or off campus. There are no upfront construction costs. The ISP may subsidize the cost of devices for the district with a longer contract.

Cons: This path can cost significantly more than others. There is no ability to contract with multiple ISPs for Internet redundancy. This path lacks the purchasing power of either RENs or district-purchased Internet access.

CONNECTING STUDENT DEVICES USING MOBILE CELLULAR BROADBAND

Located in the Sierra Nevada mountain range, Lake Tahoe Unified School District (LTUSD) is a rural district of six schools, with 60 percent of students qualifying for free or reduced-price lunch. The district found a mobile broadband solution appealing because they wanted to provide students with connectivity both at home and at school. LTUSD partnered with a commercial 3G mobile broadband provider and device vendor to supply Chromebooks to 3,000 students in grades 3-12. Each computer is equipped with Wi-Fi and a 3G wireless modem. LTUSD provides in-school and home Internet connectivity through Wi-Fi and 3G networks managed by the mobile broadband provider.

To avoid overburdening the district's small IT staff, the mobile broadband provider also provides content filtering, even when students are off campus. This vendor relationship permits LTUSD to provide connectivity to students without having to continuously update IT staff on latest technologies. While some of the materials were paid for using bonds, other components of the technology implementation, such as the connection to the ISP, were paid for using general funds, categorical funding, and E-Rate.

Major Cost Drivers

Actual network costs will vary widely from district to district based on local circumstances. The following factors will most likely have the greatest impact on the total cost of ownership:

- The number of devices and types of digital learning resources a network must support
- The capacity and age of existing physical infrastructure, including conduits, cables, and wireless access points
- The distance and geographic difficulty (terrain, weather) of connecting school buildings to the Internet
- The available Internet connection paths for joining a REN, leasing dark fiber, etc.
- The level and type of security measures needed

Two cost drivers many schools underestimate are human capital and ongoing network monitoring and maintenance. Human capital costs include the time, personnel, sustained professional development, and expertise to manage the network and provide technical support for teachers, staff, and students. Staff can also include consultants or third-party vendors that assist with technology planning, configuration, testing, and maintenance. When calculating a network's total cost of ownership, schools and districts should be sure they are comparing like services.

Ongoing network monitoring and maintenance costs can include but are not limited to the following:

- Network management and monitoring
- User help desk/technical support
- Device and equipment maintenance and upgrades
- Device insurance and service contracts
- Internet bandwidth
- Administrative software and digital learning resources
- Content filtering
- Network security
- Network redundancy

The demand for network speed and capacity will continue to increase over time. Scalability is critical. Build a network that can be improved rather than one that will require replacement as demands change. When entering a long-term contract, consider the network's maximum speed, the maximum number of devices that can be accommodated, and future Internet bandwidth needs.

SAVE COSTS AND BANDWIDTH THROUGH CACHING

One way to reduce overall bandwidth fees is to relocate content on the Internet into local caching proxies. A **cache** is a special high-speed storage mechanism that can be either a reserved section of main memory or an independent high-speed storage device. High-use content can be accessed from the cache multiple times without going back to the Internet for downloading. This tactic helps reduce costs for schools and can lower delivery costs for content providers. Caching proxies can be located within a REN, with private third-party services, or at the district level. Districts can further reduce costs by installing caching proxies within their LANs. Consider a class of 30 students, all of whom need to review the same video lesson. Instead of being downloaded 30 times, the video is downloaded once and redistributed from the local cache to each student's device.

E-Rate Funding for Internet Connectivity

The E-Rate program makes telecommunications and information services more affordable for U.S. schools and libraries. Mandated by Congress in 1996 and implemented by the FCC in 1997, the E-Rate program provides eligible schools and libraries with discounted telecommunications, telecommunications services, Internet access, and internal connections. The Universal Services Administrative Company (USAC) manages the program.

In 2014 the FCC modernized the E-Rate program, transitioning support away from legacy telecommunications technologies to advanced broadband connectivity and increasing the annual funding cap from $2.4 billion to $3.9 billion. Public, charter and private schools are eligible to apply for E-Rate funds as long as they do not operate as a for-profit business or have endowments exceeding $50 million.[30] E-Rate is one of the largest financial resources available for schools transitioning to broadband and high-speed wireless connectivity in classrooms.

The FCC adopted the following goals as part of its modernization efforts:

- Ensuring affordable access to high-speed broadband sufficient to support digital learning in schools and robust connectivity for all libraries;
- Maximizing the cost-effectiveness of spending for E-Rate-supported purchases; and
- Making the E-Rate application process and other E-Rate processes fast, simple, and efficient.[31]

To learn more about the E-Rate program, visit the USAC website at https://www.usac.org/sl/. School and district leaders should stay abreast of potential future changes to the E-Rate program to determine how they may impact technology initiatives.

Special Considerations for Rural Areas

Rural areas often have unique challenges to getting high-speed Internet to their schools. Geographic barriers such as mountainous terrain, dense forests, or swampland can make it difficult to bring wired connectivity to rural communities. Remote locations with low population densities may have difficulty attracting Internet providers. Land right usage can pose additional challenges; for example, the Navajo Nation Telecommunications Regulatory Commission noted that building the necessary physical infrastructure for high-speed Internet access was difficult due to "complications with land status, rights-of-way and building regulations."[32] These challenges can lead to schools in rural areas paying significantly higher prices per megabyte than suburban and urban schools.[33] Despite these difficulties, rural districts are succeeding in developing innovative approaches to providing teachers and students with the connectivity they need within and beyond schools.

CREATIVE CONNECTIVITY SOLUTION IN A RURAL DISTRICT

The Salamanca City Central School Districts is located on the lands of the Seneca Nation of Indians, Allegany Indian Territory, in rural Western New York State. Approximately 40 percent of the district's 1,250 students are Native American. Due to the district's rural location and high poverty rates, many students do not have Internet connectivity at home. When district leadership initiated a 1:1 mobile device program they discovered that as the initiative grew, they needed to address the challenge of providing students with Internet access outside of the school day.

In addition to working with local establishments, the district partnered with the Seneca Nation to ensure students could access their public Wi-Fi at the Administration Building, Library and Community Center. However, district officials sought additional ways to provide students with connectivity outside of the school day. Because a large percentage of students participated in athletics and other extra-curricular activities, they recognized that by adding Wi-Fi connectivity to buses, students could access the Internet and complete homework during bus rides to and from school and extracurricular events. District officials reached out to their current mobile provider to determine potential options and were able to install a cost-effective Wi-Fi solution. Overall, the initiative has been considered a success and, most importantly, students are satisfied that they can stay connected and occupied during their lengthy bus rides.

The State of Maine pays for broadband in schools using a fee of up to 0.3 percent on telecommunication services, similar to the Federal Universal Service fund, called the Maine Telecommunications Education Access Fund (MTEAF). The Maine Public Utilities Commission collects this fee on phone bills and then disperses it to the statewide broadband network to pay for the non-E-Rate portion of the cost of broadband. The MTEAF was the result of legislation passed in 1999 authorizing its creation by the Public Utilities Commission. Other states such as Georgia, Iowa, and North Carolina allow counties to enact similar paths using taxes rather than fees to finance technology for student learning.[34] Typically, the tax is for a limited number of years, after which it must be reapproved by a vote or it will expire.

MOBILE WIRELESS HOTSPOTS PROVIDING CONNECTIVITY OUTSIDE OF SCHOOL

Sunnyside Unified School District in Tucson, AZ is an example of a district pursuing strategies to connect students when they are off campus. Although 84 percent of students are low income and many lack Internet access at home, the district is one of the few in the United States to move entirely to digital textbooks.[35] To provide access, school buses are equipped with mobile wireless hotspots, enabling students to access the Internet and do homework on the way to and from school.[36] Through a partnership with the Native American Advancement Foundation,[37] the district is increasing mobile learning opportunities for children in remote villages in the nearby Tohono O'odham Indian Reservation. Sunnyside outfitted a used City of Tucson van with the same wireless hotspot equipment that is on the school buses, and the van travels daily to a new village in the reservation to provide access to students. *See Section 4: Getting Devices to Students and Teachers for more information on other strategies districts are using to increase student home access.*

Many communities have succeeded in creating low-cost fiber systems that benefit schools, local government, businesses, and residents. These involve partnering with municipal governments to engage in community-wide rollout of increased broadband access in schools, libraries, government buildings, and other public places. While these efforts can require years of coordination and planning, the costs are often offset for school districts and other local stakeholders by lower bandwidth cost once the networks come online. Collaborating with municipal governments can reduce the cost to schools and districts of establishing and maintaining broadband connections because they are shared over a wider number of users.

A number of governmental and nonprofit organizations have developed resources to assist rural communities with broadband development. The National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce, developed the BroadbandUSA initiative to provide assistance to communities that want to expand broadband capacity and promote broadband adoption. The Appalachian Regional Commission (ARC) created a Broadband Planning Primer and Toolkit that describes how other rural communities have tackled their high-speed broadband challenges and outlines a Broadband Planning Roadmap. Next Century Cities and the Schools, Health, and Libraries Coalition (SHLB) have also developed toolkits and whitepapers to assist communities with broadband deployment and adoption.

DISTRICTS AND MUNICIPALITIES BUILDING NETWORKS TOGETHER

For years, Craven County School District in rural North Carolina faced difficulties providing the connectivity required to support learning. The existing WAN and Internet connectivity could not support services such as multimedia streaming and video conferencing and the district was too far from the state's REN to make that a viable option. In 2005, recognizing that the nearby cities of Havelock and New Bern had constructed municipal fiber networks, Craven County Schools began exploring the possibility of constructing its own fiber optic network by identifying where fiber already existed in the county and potential partners. As a result, Craven County Schools initiated a partnership with Havelock and New Bern, Craven Community College, and Craven County Government to build shared infrastructure.

The local board of education agreed to fund the project as long as it found a favorable comparison between the total cost of ownership and existing leasing costs. The district of approximately 15,000 students across 695 square miles was paying nearly $350,000 per year to lease telecommunications services. The partnership achieved substantial savings by working directly with fiber manufacturers, paying $1.2 million for its 76 miles of fiber and accompanying infrastructure. In addition, the groups developed a consortium agreement and a memorandum of understanding to outline responsibilities. The project was completed within 18 months, and the network has been operational since early 2009.

3. Getting High-Speed Internet Throughout Schools

IN THIS SECTION

- Providing wireless access in schools
- Network planning
- Physical infrastructure considerations
- Network provisioning, configuration, and management
- Cybersecurity

High-speed Internet is most useful when available everywhere that teaching and learning are taking place. This section helps explain what factors are important and what questions schools and district leaders should ask before designing school networks.

Planning A Network

Within school buildings, wireless access points are the best way to connect students and staff. Wireless access throughout all learning spaces provides students and staff with mobility and flexibility when using learning devices such as tablets, laptops, and smartphones.

The first step in creating or upgrading a wireless network is to identify who will be using the network and for what purposes. This will help determine the number of connections that need to be supported, the amount of bandwidth required, and the number and placement of wireless access points. Districts lacking the internal capacity to do a comprehensive network assessment should consider contracting with external services. For more specific guidance on conducting site surveys, consult the websites of CoSN and Education Superhighway.

CONNECTIVITY DEFINITIONS

Wi-Fi is a wireless network connection using one or more of the IEEE 802.11 network specifications that carry a "Wi-Fi CERTIFIED" seal of approval from the Wi-Fi Alliance. "Wi-Fi ac" is the current generation of Wi-Fi certified devices. Devices with a "Wi-Fi CERTIFIED n" designation are from the previous generation, meaning they are slower than ac devices). A Wi-Fi channel is one frequency within the Wi-Fi spectrum. Most Wi-Fi networks have approximately 11–15 channels.

A **wireless access point** (AP) is a device that allows wireless connections to a wired network using Wi-Fi or a related standard wireless network protocol.

Ethernet is a family of networking technologies for LANs. Ethernet standards are most commonly provisioned with twisted-pair and fiber optic cable. When twisted-pair is used, CAT 6a cabling is required to support speeds up to 10 Gbps. The most popular Gigabit Ethernet fiber optic standards are the 1000BASE-SX and 1000BASE-LX standards.[38]

Because wireless signals are influenced by environmental factors such as radio frequencies, electrical interference, and building design and construction, the placement of access points is important. Check for interference at different times of day and on different days. In addition, consider testing some of the actual devices that will be used by students and staff to gauge performance.

COUNT ALL DEVICES

As Burlington High School in Burlington, MA prepared to provide mobile devices for just over 1,000 students, school staff did their homework in creating a wireless infrastructure. A vendor completed a network assessment to provide the school with the correct number of wireless access points for the 360,000-square-foot campus.

On the first day of school, however, Burlington's CTO came to the quick realization that students' personal devices had not been considered in the network assessment. Burlington was not actually a 1:1 school, but a 2:1 or even 3:1 school when considering all the personal devices being used on the network. This created limited access to the network and was particularly problematic for classrooms near the cafeteria, where 500 students regularly attempted to access Wi-Fi during lunch from their personal devices. District IT staff were able to make the necessary adjustments to wireless access points to support the actual number of devices. Burlington's experience offers an important lesson: consider every device that will be using the network, not just the devices provided by the school.

Consider All Physical Aspects of the Network

There are a number of components to consider when planning to create or upgrade a network, including:

Electricity—What elements of the network require external power? How many outlets are required to meet these needs? Will a generator be necessary to support the network in the case of a power outage?

Cabling—Where will access points be installed, and what cabling is needed to connect them?

Access points—Who will conduct the site survey to determine both the number and types of access points? Will a consultant assist with this process? Configuring network hardware for use with wireless access points requires considerable expertise. Although one access point per classroom is a frequent recommendation, the precise number will depend on the hardware selected. Larger rooms (e.g., cafeteria) will require more than one access point.

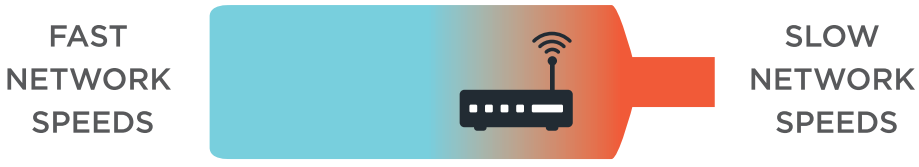
DETERMINE WIRING NEEDS

Internal network cabling is necessary to distribute high-speed broadband throughout a school building. Fiber or CAT 6a cabling is recommended. Cables designed to be run through drop ceilings (known as plenum cables) are subject to special fire-safety standards for flammability and smoke density. Installing network cable is a technical job that is often subject to local and state electrical building and fire codes. Cabling should be professionally installed and communications closets should be kept secured. A licensed electrical or telecommunications contractor can provide advice regarding relevant building codes.

THE SPEED OF THE ENTIRE NETWORK MATTERS

To get high-speed Internet connectivity to classrooms, every segment of the network must be able to accommodate high speeds. No matter how fast the Internet connection, user experience will be poor if the network inside the school is outdated. The slowest segment of a network determines the speed of the network downstream from that point. It may be helpful to think of a network as a multi-lane highway; if a segment of the highway is reduced to one lane, traffic will slow to a crawl. Routine inspection and continuous network monitoring will help identify misconfigured and/or failing equipment, inferior or damaged cables, or radio interference that is causing dropped connections. Internal or consulting IT experts can help schools and districts define a strategy that best fits their individual organization.

High-speed connectivity can be affected by old infrastructure.



A slow router can significantly slow down the speed of your network.

CONSIDER PHONE REQUIREMENTS

Consider the technology used for voice communications when planning a network. Voice over Internet Protocol (VoIP) technology enables schools to provide phone service over the same network used for Internet access. This approach eliminates the need for maintaining a separate phone system and can reduce the amount of cabling needed throughout the building. Schools planning to support VoIP should factor in the additional network capacity and cabling required. In addition, for emergency service providers (such as 911) to determine the location of calls made over VoIP, the address of the phone must be registered manually. Schools using VoIP phones must ensure their provider properly registers the physical location information of handsets with the E911 registry.

INCLUDE SECURITY SYSTEM REQUIREMENTS

Many security systems such as security cameras capture video that travels across a school network and use bandwidth. Other systems such as fire or intrusion detection use IP-based monitoring as opposed to traditional POTS (Plain Old Telephone Service) lines. Be sure to take these systems into account when planning internal networks.

IMPORTANT QUESTIONS TO ASK

When designing a school network, consider the following:

Intrusion detection—Are monitoring systems in place to identify malicious software activity and unauthorized network access? Do these systems notify key personnel after hours?

Security—Is network equipment secured and kept safe from theft, vandalism, and physical or virtual hacking? Are security processes and policies documented and regularly maintained?

Firewalls—Can IT staff restrict what data enter and exit the school network? Are enterprise-level systems in place to detect unsolicited and unwanted email and prevent those messages from getting to user inboxes?

Load balancing—Can network resources scale to meet student and staff needs?

Content filtering—Are tools in place to restrict access to inappropriate content while still permitting access to learning tools?

Network management—Are systems in place to monitor network traffic and push out software updates to networked devices?

Uninterruptible Power Supplies (UPS)—Are key network appliances connected to UPS equipment designed to protect from power surges and allow controlled server shutdowns in the event of an extended outage?

Mobility—Is the network configured so that students can remain connected even if they move to different physical locations in the building? Does the wireless network provide adequate coverage throughout the campus? Is it able to handle high-density usage, such as a class of students using mobile devices simultaneously?

User logins—Will users need to log in to access the network? Does the network hardware support the kinds of login services you want to offer?

NETWORK MANAGEMENT TERMS

Content filtering is the ability to screen content traveling over the network in real time and restrict access. For example, almost all schools filter access to websites known to contain inappropriate content. Whitelisting is the practice of explicitly allowing access to a particular site or service, which can include allowing emails from a specific domain, sender, or IP address to be delivered. Blacklisting is the practice of explicitly blocking such access.

A **firewall** acts as a network gatekeeper, restricting access into and out of the network based on a predefined policy. Firewalls can be hardware appliances, software, or both.

An **intrusion detection system (IDS)** is a service used to identify security threats within a network. These solutions alert the operator to suspicious files, processes, and configurations on a network.

Load balancing improves network performance by distributing network traffic and processing evenly across a network so no one single device is overwhelmed. This allows for more efficient use of bandwidth.

Login services validate identity so a user can gain access to a computer system or other technology.

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, and maintenance of networked systems. This includes the management of access points and other devices that constitute the network.

Quality of service (QoS) is the practice of prioritizing certain types of network traffic. An example would be prioritizing network traffic associated with online assessments and learning management systems over that of general web browsing. Implementing QoS ensures users have high-quality and prioritized access to important content.

Configuring and Managing A Network

Planning for network configuration and management will better position technology staff to respond to issues as they arise. The following section provides guidance on what features and services schools and districts should consider.

In most situations, enterprise-grade equipment is needed to support modern digital learning environments. Small office or home office-grade equipment may be less expensive, but will not offer the features needed to support mobile devices at scale. Features to look for include:

- Remote device management and access
- Centralized login support
- Per-user VLAN routing

SOHO FOR MOBILE LABS

Compared to commercial-grade equipment, an unmanaged small office/home office (SOHO) wireless access point might be acceptable for a laptop cart, in a mobile lab where equipment is moved around frequently, or for an ad hoc event like providing a temporary wireless bridge for a sporting event. If using a SOHO in addition to a main network, ensure filtering and security settings are in place.

Connectivity plans should include a comprehensive network monitoring service. A good monitoring system analyzes information such as:

- Network traffic and saturation
- Time and conditions of peak network use
- System-wide status and capacities such as detecting when a service (e.g., VoIP) is failing or when network storage needs expansion or archiving
- Unreachable or misconfigured devices

Most servers, routers, and wireless access points need to be refreshed every 4 to 6 years. Be sure to plan for network equipment upgrades when developing budgets. Hardware that can be centrally managed and configured saves time and frees up staff resources for other tasks.

PRIORITIZING TRAFFIC

Prioritizing certain types of network traffic can help maximize the use of available bandwidth. For example, a school or district might prioritize the bandwidth needed for testing or other classroom use. IT staff can also prioritize traffic to and from specific websites based on the instructional value.

In addition to providing access to school-owned devices, schools and districts may consider providing access for student and staff personal devices or public guest access for school visitors. For example, there may be a BYOD network for students, faculty, or guests that is separate from the wireless network used by school-owned devices. Segmenting networks prioritizes student and staff access and improves network security.

Some schools segment their network in ascending order of priority: high-priority traffic (e.g., testing), normal classroom traffic, BYOD traffic, and public guest traffic. Providing public guest access will make the wireless infrastructure design more complex due to the need for additional security and authentication.

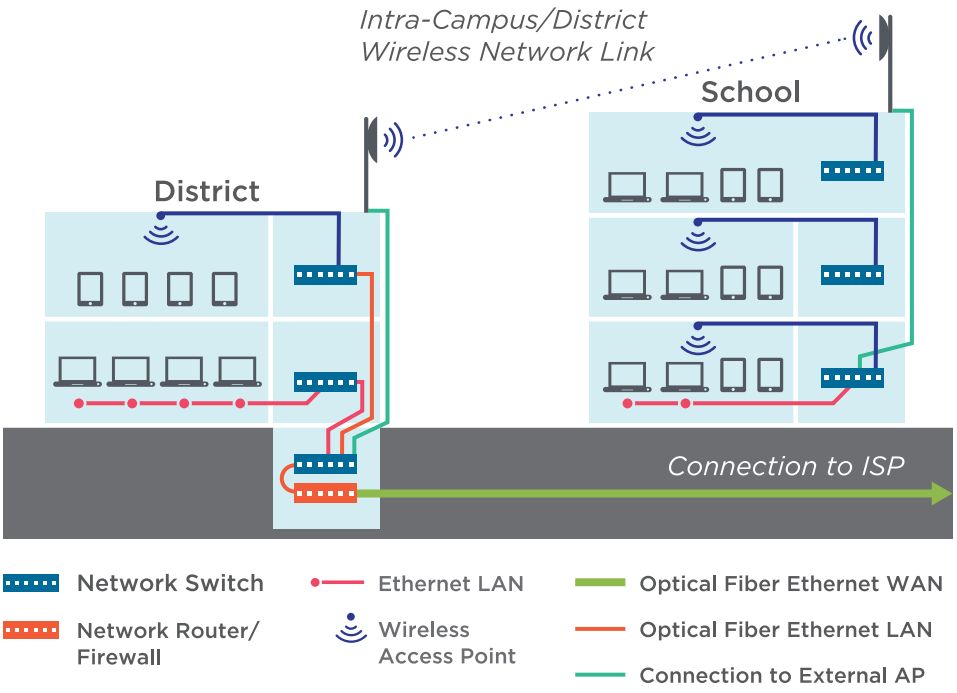
SEGMENTING NETWORKS TO ALIGN WITH LEARNING PRIORITIES

Fairfax County Public Schools (FCPS) in northern Virginia has a dedicated network for BYOD devices. FCPS has over 200 schools and centers serving 185,000 students and more than 30,000 staff, and provides public Wi-Fi access in all facilities. The district configured its network into three segments to support this large number of users. Students use the FCPSMobile configuration by authenticating themselves to the network using their student ID and password. Once authenticated, students have access to filtered high-speed Internet, intranet resources, print and file share services, and learning resources. The FCPS staff accesses the secure FCPS network, which provides additional access to intranet and business systems like the student information system, online testing, human resources, and financial systems. The public FCPS access provides filtered broadband but no access to the FCPS private intranet. By segmenting the network, the district can prioritize the most important network traffic.

Traffic peaks often occur at certain times of day, such as when students log in at the beginning of each instructional period. Track both upload and download speeds when monitoring network traffic peaks. Be sure the network can handle the extremes of user demands rather than the average.

The illustration below provides an example of connections that can be used to extend high-speed connectivity throughout a school campus.

CONNECTING THE CAMPUS



Cybersecurity

Cybersecurity breaches and attacks are impacting schools and districts with increasing frequency. Data breaches, whether caused by human error, theft, or hacking pose great financial and legal risks for schools. Distributed Denial of Service (DDoS) attacks, in which outside systems coordinate to overwhelm the bandwidth or resources of a targeted system have made headlines for disrupting online testing. Malware, ransomware, and social engineering attacks can put student and employee data at risk and significantly disrupt school operations. When installing, operating and maintaining, or upgrading a network, it is critical to assess the risks and prepare for wide range of cyber threats, whether they are caused by physical intrusion, virtual attacks, or human error.

Inadequate funding can exacerbate existing cybersecurity risks and leave staff underprepared to meet future threats. Nearly half of districts surveyed in 2016 reported spending less than 4 percent of their technology budget on cybersecurity. Almost 20 percent of schools and districts reported spending less than 1 percent. Only 42 percent of school and district technology leaders believe their organizations take a proactive or very proactive approach to addressing cybersecurity.[39]

CYBERSECURITY FRAMEWORKS

Cybersecurity should be considered within the larger framework of school and district emergency preparedness activities that address security, safety, and emergency management. In the same way that schools and districts develop business continuity plans to protect personnel and assets during a physical disaster, they should identify, assess, and prioritize mitigation strategies for cybersecurity attacks. The National Institute of Standards and Technology (NIST) released their updated Framework for Improving Critical Infrastructure Cybersecurity which provides voluntary guidance to organizations on reducing cybersecurity risks. Designed to complement existing business and cybersecurity operations, it can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing one. The five core functions of the framework—Identify, Protect, Detect, Respond, and Recover—organize basic cybersecurity activities at their highest level. These functions are then divided into categories and subcategories tied to programmatic needs and specific activities. The framework is designed to be flexible and customizable to the current priorities and risk disposition of individual organizations.

INTEGRATING CYBERSECURITY WITH EMERGENCY OPERATIONS PLANNING

Check out the Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center's webinar with the U.S. Department of Education's Office of Safe and Healthy Students and the U.S. Department of Homeland Security's Office of Cybersecurity and Communications on Integrating Cybersecurity with Emergency Operations Plans for K-12 Schools, along with the Resources page on the REMS TA Center website, which houses resources on key emergency management topics including cybersecurity.

The Consortium for School Networking (COSN) has assembled a cybersecurity toolkit that takes schools and districts step-by step through the process of cybersecurity self-assessment, planning, and risk mitigation. The toolkit includes a school/district self-assessment checklist, a security planning rubric that helps school leaders determine their current degree of cybersecurity preparedness, and a security planning template to help schools and districts prioritize cybersecurity

improvements. As schools and districts conduct the cybersecurity self-assessment, they may also want to incorporate the findings from a site assessment or vice versa. A site assessment examines the safety, accessibility, and emergency preparedness of district or individual school buildings and grounds.

FREE CYBERSECURITY SERVICES FROM THE DEPARTMENT OF HOMELAND SECURITY

The **National Cybersecurity Assessments and Technical Services (NCATS)** team is a division of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). NCATS has three primary service offerings that are available to schools and districts at no cost: Cyber Hygiene, Phishing Campaign Assessment, and Risk & Vulnerability Assessment.

Cyber Hygiene (CyHy) is a scanning service intended to help organizations follow best practices and eliminate known vulnerabilities from your Internet-facing systems. A report of the findings is delivered weekly. Once initiated, this service is mostly automated and requires little direct interaction between NCATS and the school or district.

Phishing Campaign Assessment (PCA) measures a team's propensity to click on email phishing lures, commonly used as a means to breach an organization's network. PCA results can be used to provide guidance for anti-phishing training and awareness.

A **Risk & Vulnerability Assessment (RVA)** is a dedicated, customizable two-week engagement that allows schools and districts to select from a menu of network security services including penetration testing, network mapping and vulnerability scanning, phishing, and/or web application and database security assessments.

For more information, email ncats_info@hq.dhs.gov.

COMMON CYBERSECURITY THREATS

Phishing is an attempt to gather confidential information from unsuspecting users, typically by sending an email that looks like it comes from a legitimate institution, such as a bank. When users click on attachments or links within the email, their computers can be infected with malware and/or users can be sent to fake websites that resemble the real ones and may collect sensitive user information. Twelve percent of school technology leaders in 2016 reported receiving phishing attacks daily, with twenty percent receiving them weekly.[40] Spam filters are programs used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. While they may block unsophisticated junk mail and some malicious content, they are not as effective at catching sophisticated phishing emails.

Spear phishing attacks use social engineering to focus on specific individuals or employees within an organization by specifically customizing accurate and compelling emails based on user data. Users whose jobs involve sensitive information or financial data such as human resources and payroll are at particular risk. Spear phishing attacks are growing increasingly sophisticated. Some schools and districts engage third parties to send simulated phishing attacks to assess user ability to identify and avoid phishing emails.

Business email compromise (BEC) is a sophisticated email scam in which fraudsters impersonate high-level executives to trick a target into sending money to an attacker's account or access confidential financial data. The scam may incorporate spear phishing as the attack vector. An example would be the W-2 scam targeting schools and other businesses.[41] Users are particularly vulnerable to this attack because of the apparent involvement of supervisors or senior leadership.

Ransomware is computer malware that installs itself on a user's computer and prevents users from accessing their data through encryption or threatens to release private or sensitive data publicly unless a ransom is paid. On a school network, ransomware can spread to shared network resources such as file servers and hold an entire organization's data hostage. Some districts have been forced to pay thousands of dollars to retrieve their data or rebuild the school or district's data systems from backups or, in a worst-case scenario, from scratch.[42] Even if the data is recovered, it is often unclear if it has been captured or copied by malicious actors.

Lost/stolen mobile devices (such as laptops and smartphones) containing unencrypted confidential data can cause data breaches when they are stolen or lost. Full disk encryption, especially for school and district employees who work with highly sensitive data, is an effective and low-cost strategy that can help prevent data loss. Mobile device management solutions that allow for the remote locking and wiping of devices can provide additional security.

Employee negligence Data breaches or information theft can occur when employees have unnecessary access to information or when access isn't terminated when an employee resigns. Other common employee mistakes can include sending sensitive data to the wrong person, using weak, stolen/shared, or default passwords, or improperly storing and disposing of confidential paper and electronic data.

Hacking is an unauthorized intrusion into a computer or network. In a 2016 CoSN survey, two-thirds of school and district technology leaders reported foreign hackers as the primary attackers, followed closely by cybercriminals (42 percent) and then students (31 percent).

A comprehensive cybersecurity plan should be incorporated into an overall school or district emergency operations plan (EOP) and take into account the three pillars of people, policies, and technology as well as the goals, objectives, and activities/courses of action for before, during, and after a cybersecurity incident. When developing a school and/or district EOP that address cybersecurity, planning teams should take the following actions during each step of the six-step planning process for EOP development outlined in the federal *Guide for Developing High-Quality School Emergency Operations Plans (School Guide)*.

GOAL OF STEP IN SIX-STEP PLANNING PROCESS FOR EOP DEVELOPMENT	CYBERSECURITY-RELATED ACTIONS
Step 1: Form a Collaborative Planning Team	Designate personnel who have a role in both cybersecurity and in managing cyber incidents or emergencies.
Step 2: Understand the Situation	Identify cyber threats and hazards. Assess the cyber risk. Identify the cyber vulnerabilities.
Steps 3 & 4: Develop Goals, Objectives and Courses of Action	Develop goals and objectives for each cyber threat identified in Step 2. Develop a variety of measures to prevent cyber threats. Highlight action steps to address cybersecurity overlap with other action steps to address other emergencies. Categorize action steps into a Cybersecurity Annex or a cyber threat- and hazard-specific annex.
Step 5: Plan Preparation, Review and Approval	Address how the annex connects to state/county/municipal plans. Identify chain of command. Identify contact information for key staff. Clearly identify roles and responsibilities.
Step 6: Plan Implementation and Maintenance	Train stakeholders on the plan to address cybersecurity. Conduct emergency drills and exercises related to cybersecurity. Conduct after-action reviews of both drills and actual cyber incidents. Identify lessons learned and implement corrective actions.

Schools and districts should allocate adequate cybersecurity funding to identify and mitigate potential vulnerabilities in all areas.

People: It is critical for schools and districts to build the cybersecurity capacity of both technology personnel and end users. Skilled data security personnel are in high demand and can

command much higher salaries in industry than many schools and districts can afford. While outside consulting services can help bridge the gap, schools and districts should invest in technical staff to ensure their IT security skills are kept current. It is also important for schools and districts to educate faculty, staff, and students about best practices in cybersecurity and data protection. Training users to create complex passwords, identify phishing emails, and recognize suspicious websites can pay huge dividends in network security. Additional training about specific federal and state privacy legislation impacting education and basic data security best practices can help prevent the inadvertent release of confidential information. Most important is developing a culture that emphasizes the thoughtful implementation of security policies rather than mere compliance—a culture in which cyber- and data security are seen as a community responsibility. A well-trained and security-aware workforce is one of the best defenses organizations have against data breaches and malicious attacks. Similarly, it is critical to provide students with training.

MAKING EMPLOYEE CYBERSECURITY EDUCATION A PRIORITY

The Madeira School in McLean, VA decided to make employee cybersecurity education a priority after 40 percent of its employees "fell" for a simulated phishing attack sent by an outside security vendor contracted by the school. Further data analysis showed that 80 percent of new employees (hired within the past year) fell for the phishing simulation. Jeff Dayton, Director of Technology and Innovation, immediately began working with the human resources department to incorporate cybersecurity training into the new employee onboarding process and teacher professional development. He created a cybersecurity-focused intranet website for employees that houses the school's technology and data security policies and contains links to videos, news articles, and other cybersecurity education resources. Dayton also conducted an internal cybersecurity audit using an auditing checklist available online to identify security gaps with regard to policies and technology. He is using the audit results to systematically mitigate potential security risks.

Dayton began publishing a weekly email security newsletter for faculty and staff, drawing topics from the week's headlines and conversations with staff. For example, during March Madness, he wrote about basketball tournament-related cyber scams. By relating content to current events and their personal interests, Dayton finds that users are more likely to engage with the shared resources.

Policies: Clear and well-communicated policies around cybersecurity and data privacy are another important component of a well-implemented security program. These include policies addressing technical practices such as network security and access control, data backups and retention, password management, mobile device policies, and incident response as well as policies regarding such topics as confidential data access, data transfer, data sharing, and encryption. Schools and districts that accept credit cards may have to develop additional security policies and procedures, such as those for Payment Card Industry Data Security Standard (PCI-DSS) compliance.

Policies should be reviewed and updated on a regular basis and outlined in a school or district's cybersecurity plan or cybersecurity annex that is part of a larger Emergency Operations Plan. Inform employees and users about policy requirements. Be sensitive to the fact that policies that make sense on paper may present challenges in practice in an educational environment. Balancing these security considerations with educational needs and impact to students and

faculty is critical. For instance, complex password requirements that are considered best practice for adult users may not make sense for young elementary students with limited keyboarding skills or for students with attention issues or cognitive disabilities.

USING 2-FACTOR AUTHENTICATION TO IMPROVE SECURITY

Two-factor authentication (2FA) is an extra layer of login security that requires not just a username and password, but an additional authentication factor such as answering a security question or entering a code sent via text message or email. This provides an extra layer of security in case a username and password are compromised. Many commercial web applications such as banking websites require or allow users to use two-factor authentication to decrease the risk of account compromise.

In recent years, the Anchorage School District in Anchorage, AK has seen a steady increase in the number of sophisticated phishing attempts against staff. Although professional development and information security awareness helped reduce the effectiveness of phishing, the district sought to implement additional strategies improve data security. They decided to transition to two-factor authentication for staff users connecting to certain school resources through a **virtual private network** (VPN). VPN encryption enables computers to connect to each other across a public network as if they were connected on a private, secure network. Requiring two-factor authentication for VPN login provides an additional layer of security for users accessing certain legacy applications that contain sensitive data. Staff can opt to use a variety of methods for the second authentication factor, including receiving a telephone call or text message or using a mobile app. Instructions are provided by streaming video.

Technology: Technical protection measures are the third prong of a robust cybersecurity program. Hardware appliances and software applications such as firewalls, intrusion detection systems, enterprise antivirus, managed software patching and update services, spam filters, advanced behavioral protection, and mobile device encryption are just a few of the technical components essential for maintaining network security. Advanced threat protection technologies including exfiltration prevention, behavioral sandboxing and selective decryption should also be considered along with strategies such as network segmentation. Security audits and assessments, including capacity assessments designed to examine internal capabilities as well as the services and material resources of community partners on the local, state and federal levels, can be conducted as a part of the cyclical EOP development and planning process. Learn more about conducting assessments as a part of Step 2 in the six-step planning process for EOP development via the *School Guide*, which can be accessed via the Readiness and Emergency Management for Schools (REMS) Technical Assistance Center website.

IMPROVING DATA SECURITY THROUGH AGENCY PARTNERSHIPS

Orange County Public Schools in Orlando, FL, is the 9th largest school district in the country. Recognizing that it was essential to focus formally on data security, OCPS designed and built a data security program to provide a secure computing environment for nearly 200 schools and protect the personally identifiable information (PII) for 24,000 staff and over 203,000 students.

The district knew that the design, recruitment, and development of the data security program would require funds for hardware, software, and staff with the necessary security credentials. Data security personnel are scarce, extremely sought after in the private sector, and require salaries above and beyond what typically is offered by a school district's personnel office. To address staffing needs, IT department leadership assessed the existing skill sets, abilities and credentials of OCPS technology personnel. Based upon personal aptitude, a desire to learn, and willingness to re-tool skill sets, they then selected and formed a team whose members were assigned specific information security-related tasks.

Because an infrastructure assessment was required to build a computing environment that would minimize organizational risk, the district partnered with the Department of Homeland Security's National Cybersecurity Assessments and Technical Services (NCATS) team. NCATS staffers performed a free cyber hygiene assessment that resulted in the identification of 30 critical and high vulnerabilities. Results from the cyber hygiene and staff assessments enabled the district to build a business case for the Data Security program to be included in future budget forecasts. Senior district leadership approved the business case along with funds for continuance of the program.

By partnering with other agencies that have strengths in data security, OCPS was able to build its Data Security program while minimizing costs, strengthening the skillsets of existing staffers, and building community relationships. OCPS continues to build partnerships with the local community agencies including city, county, and law enforcement.

Because traditional commercial general liability and property insurance policies typically exclude cyber risks from their terms, schools and districts may wish to consider purchasing **cyber insurance**, which can help mitigate risk exposure by offsetting the costs involved with recovery after a cyber-related security breach or similar event. The reimbursable costs can include forensics investigations, business losses, privacy notification and credit monitoring for individuals impacted by a data breach, and legal expenses.[43] Some schools and districts require third party contractors to have cyber insurance as well.

No matter how strong the safeguards, no network is impenetrable and even well trained employees make mistakes. As a part of school and district emergency operations planning, school leaders should 1) develop a cybersecurity plan, 2) share the information with stakeholders (including community partners, such as law enforcement) and train them on their roles and responsibilities, and 3) conduct exercises to test the plan and the school's ability to respond to an incident. All these activities should be conducted while keeping in mind the inadvertent or malicious disclosure of private data that may occur. See PTAC's Data Security Best Practices and Data Breach Response Checklist for guidance in protecting against and dealing with unintended and malicious data disclosures. *See Section 5: Responsible Use, Privacy, and Other Considerations for more guidance on privacy and protection considerations.*

4. Getting Devices to Students and Teachers

IN THIS SECTION

- Importance of devices in digital learning environments
- Considerations when selecting devices
- BYOD programs
- Funding strategies
- Device maintenance and management
- Home access
- Rollout models

The educational benefits of increased connectivity can only be maximized when teachers and students have 1:1 access to mobile devices. Shared devices make it difficult for students to engage in "everywhere, all-the-time" learning and limits access to personalized learning opportunities targeted to their interests, experiences, and needs. Moreover, many states have college- and career-ready standards that require students to possess certain digital literacies and competencies to prepare them to thrive in a connected world.

Districts are increasingly adopting web-based productivity tools and digital teaching and learning content. These shifts to web-based materials and tools can decrease paper usage, make more efficient use of teacher time, and enable students and teachers to access learning materials at any time of day.

Considerations For Device Selection

The primary driving factors in device selection should be learning objectives and the school or district vision for technology-enabled learning.

Test several devices before making a commitment. Create a test script or a list of actions for teachers and students to try on each device. Be sure that devices are compatible with web-based platforms, online curriculum, or electronic textbooks used by the school or district. Do not compare devices by technical specifications alone or be swayed by vendor sales pitches. The ability of devices to enhance student learning should always be the main evaluation criterion, and getting them in the hands of students and teachers is the best way to test this.

Accessibility issues are particularly important when considering which devices will best serve students' learning needs. Special education specialists should be an integral part of the device selection process. The Individuals with Disabilities Education Act (IDEA) requires that children with disabilities have access to the general curriculum and that they will receive the services and supports needed to achieve their educational goals and prepare them for further education, employment, and independent living. To meet their educational goals, children with disabilities must have full access to the general education curriculum. Further, Section 504 of the Rehabilitation Act of 1973 (Section 504), prohibits discrimination on the basis of disability in programs or activities receiving Federal financial assistance, such as public schools. Title II of the Americans with Disabilities Act of 1990 (Title II) prohibits discrimination on the basis of disability by public entities, including public schools regardless of the receipt of Federal financial assistance. Schools must take into account the requirements of Section 504 and Title II when making technology-related decisions.

Assistive and instructional technologies, which may include software, devices, and accessible versions of curricular materials, textbooks and media, are powerful tools that can ensure full access to educational curricula and content. The Individualized Education Program (IEP) for a child receiving special education and related services under IDEA or a plan for students receiving educational and related services under Section 504 can and often does include specific content about the child's educational technology needs and how those needs will be met. Hardware, software and accommodations may be addressed in a child's IEP or plan under Section 504. When selecting devices and learning technologies, be sure to coordinate with the school and district staffers who are most familiar with accessible devices and technologies generally and those familiar with individual student accessibility needs. Third party consultants may also be helpful. For more information about assistive and instructional technologies, media and accessible educational materials, visit the Center on Technology and Disability and Bookshare.org.

As with networks, it is important to **compare the total cost of ownership for devices and peripherals**, including keyboards, protective screens, cases, and software. A cheap device that requires an expensive protective case may cost more in the long run than a slightly more expensive but more durable device.

Computing devices most frequently come in four different types: desktops, laptops, tablets, and smartphones. Generally, laptops or tablets are school deployment devices of choice because they are portable, have large enough screens for most activities, and are relatively affordable. Some devices incorporate features of both laptops and tablets.

Districts may consider involving a variety of stakeholders in device selection. For example, in Rhode Island the devices used in the Chariho Regional School District's 1:1 initiative were chosen by a Device Selection Advisory Committee composed of administrators, superintendents, school committee members, teachers, students, the director of technology, and a community member.[44,45] Stakeholder inclusion can help inform decisions and bolster community support during technology plan implementations.

Ask these questions when evaluating devices:

- For what tasks will the devices be used?
- Does battery life live up to expectations?
- How durable are the devices?
- How important are considerations such as screen size, keyboard/mouse, and peripherals such as scientific probes?
- What are the most developmentally appropriate options, given the age of the students who will be using the devices?
- Are the devices accessible to individuals with disabilities?

Here are some factors to consider during the device evaluation process:

1. Tablets

Pros: Tablets tend to be lighter and offer a touch screen interface, which can be particularly useful for younger learners. They may have longer battery life than some laptops models. Peripherals such as science probes can complement tablet mobility, making possible lab experiments in the field.

Cons: Tablets may not come with keyboards, which can make longer writing assignments challenging without the purchase of an external keyboard. Not all learning resource providers have updated their products for tablet use, which can adversely affect functionality and interactivity.

2. Laptops

Pros: Laptops have built-in keyboards and may have larger displays and more processing power. Some devices combine the functionality of a traditional laptop and a tablet. Laptops are compatible with a wide range of digital learning resources and educational software. Some laptops, for example, Chromebooks have a web-based operating system that relies largely on cloud-based file storage.

Cons: Depending on the model selected, laptop battery life may be shorter than that of tablets. Their size can potentially limit mobile use.

Determining Device Specifications

Device specifications should be based on their intended use. Computers that will be used with high-end engineering or graphic design software, for example, will need larger screens and considerably more memory and processing power than devices to be used for word processing and web browsing. Be sure to consider requirements for assessments that may be delivered on the devices. Many online assessments specify minimum screen sizes, speed, and keyboard and/or mouse requirements. Individual assessment websites will list the specific technical requirements for student devices.

Purchasing devices that barely meet minimum specifications for delivering assessments may not be in the best interest of a school or district's broader educational goals. Consider optimal rather than minimal standards because they will provide better performance. A 9-inch screen may meet the minimum threshold for online assessments, but will it best serve other educational needs? This does not mean that schools and districts should feel compelled to purchase the latest and greatest. For example, San Diego County purchases devices that fall in the 55–75 percent range of premium (0 percent being the minimum specification and 100 percent being the most

above-specification technology). By using this strategy, the county purchases devices that provide acceptable performance and are reasonably priced.

USE SINGLE SIGN-ON WHEN POSSIBLE

Single Sign-On (SSO) is a user authentication process that enables users to access multiple applications by entering just one name and password. This reduces the number of login credentials that users must remember, simplifies technology management, and helps minimize lost instructional time caused by forgotten user credentials.

Bring Your Own Device (BYOD)

BYOD policies can provide students with greater choice and control of the technology they use. However, schools should proceed carefully when considering BYOD as a replacement for school-provided devices, as these policies can create several challenges:

Economic disparity—The ability to access digital learning materials is disproportionately distributed to students whose families can afford the devices. This can widen the very learning gaps that technology is capable of closing. It may also raise legal concerns because schools are expected to provide a free education for students. If devices are required materials, all students must have access to comparable devices.[46] Schools should be prepared to provide devices (and possibly home internet access) for students who cannot afford them.

Instructional burden—It can be difficult for teachers to manage learning activities when they have to support multiple platforms and devices, as some activities may be incompatible with certain devices. Schools may wish to require students who bring their own devices to meet certain minimum technical specifications and/or have school-provided devices available for students whose devices are not compatible with specific learning activities.

Assessment security—Student-owned devices may not have the functionality necessary to support a secure testing environment. For schools or districts that utilize online assessments, student-owned devices will most likely not provide an acceptable assessment option.

When considering allowing BYOD, be sure to consider the following points:

- Implement security measures (such as content filtering) at the network level rather than at the device level. Network segmentation can help minimize the security risks posed by student-owned devices.
- Use cloud-based resources when possible.
- Ensure online learning systems support the use of personal devices.
- Set minimum device requirements for BYOD devices or provide a list of preferred devices. This can help standardize the device environment.
- Consider strategies to ensure that students who cannot afford to bring their own devices still have access to high-quality devices.

POWER UP AND BRING YOUR OWN DEVICE

The educational leaders at Forest Hills School District in Hamilton County, OH believe that learning should take place everywhere and all-the-time. Realizing that existing district-owned tools could be leveraged in combination with student-owned devices, they launched their Power Up Bring Your Own Device program. Students in grades 6-12 are required to bring their own device while grades 2-5 have 1:1 school-provided devices. Students without their own device receive one from the district. The district held a parent night run by students to showcase their devices and address any community concerns. Teachers provide additional training to parents and students on the learning management system and other technology tools used during the school year. Forest Hills School District also partners with Cincinnati Bell Technology Services to provide parents with monthly cyber education opportunities and trains teachers on how to effectively use technology to engage students in learning.

Forest Hills district leaders also understand that the professional learning landscape is changing for faculty. Recognizing that teachers can also benefit from personalized learning, they are expanding professional development opportunities beyond face-to-face sessions. Flexible learning opportunities for teachers include webinars and a summer learning series. Forest Hills was chosen as one of four schools in the United States to be leaders in the "connected educator" space. Their BYOD and 1:1 initiatives continue to evolve into more blended and personalized learning models.

Structuring Device Purchases

This section highlights three funding strategies commonly used by schools and districts across the country.

Outright purchase—Through outright purchase, a district buys and owns the devices until it decides to retire them via donation, salvage, or other disposal method. With this model, districts may purchase a warranty or service agreement from the manufacturer or retailer to repair or replace devices under certain circumstances. Although this can expedite purchasing, schools or districts that do not create a yearly budget line item for device upgrades may lack funding for the replacement of end-of-life devices. Some districts establish this line item as the result of amortizing a purchase across multiple fiscal years through the selling party or a third-party lending institution. This allows for outright purchase in schools and districts that do not have budgets allowing for a single bulk payment.

Unfortunately, devices purchased outright may be deployed to students and teachers for longer than 3-5 years. As a result, students end up using outdated technology and IT departments are faced with higher labor and maintenance costs. Before leveraging nonrepeating funds for an initial technology purchases, determine how to fund future device replacements.

Leasing—In a leasing model, schools and districts lease devices over an extended term instead of purchasing them outright. The leasing company owns the equipment and provides upgrade options based on the agreement terms. For example, a district that enters into a 3-year lease agreement has the option to upgrade the devices at the end of the lease. Relative to outright purchase, leasing addresses some of the challenges created by owning equipment, including regular budgeting, maintenance, and equipment replacement.

Cooperative purchasing—With cooperative purchasing, school and districts may be able to purchase equipment through regional, state, or consortium-based purchasing contracts. These

contracts can offer volume-purchase and discount pricing for individual schools or smaller-to-medium-size districts. State education authorities can provide information on available consortium purchasing in individual states.

Organizations should consider putting out a Request for Proposal (RFP) for major purchases. RFPs make vendors compete for business, leading to more competitive pricing.

Funding Device Purchases

In addition to the possible funding sources outlined here, schools and districts should adopt the mindset that technology purchases are a normal part of school operations and should be considered recurring expenses within the budget.

In October 2016 the U.S. Department of Education released Non-Regulatory Guidance: Student Support and Academic Enrichment (SSAE) Grants. This grant program, newly authorized by the ESEA as amended by ESSA, focuses on activities to support well-rounded education, safe and healthy students, and the effective use of technology. This guidance highlights some of the ways that SSAE funds can be used to improve the effective use of technology, including building technological capacity and infrastructure.

Local Education Associations (LEAs) may use SSAE funds to build technological capacity and infrastructure by purchasing devices, equipment, and software applications to address readiness shortfalls. Districts may not use more than 15 percent of the funds provided under section 4109(a) for this purpose.[47] See the non-regulatory guidance on Title IV, Part A for more information as well as the webinar, "ESSA, Title IV, Part A: Allowable Activities to Support Well-Rounded Educational Opportunities; Safe and Healthy Students; and the Effective Use of Technology."

In addition, a U.S. Department of Education Dear Colleague letter published in November 2014 and updated in January 2017 provides guidance and examples for leveraging existing federal funds for technology-related expenditures. The examples provided in the letter clarify opportunities to use federal grant funds to support digital learning, including improving and personalizing professional learning and other supports for educators, increasing access to high-quality digital content and resources for students, facilitating educator collaboration and communication, and providing devices for students to access digital learning resources. The breadth of allowable uses of the funds recognizes that technology itself is not sufficient to improve student performance; it also requires supporting actions and activities.

Some school districts leverage short- and long-term bonds approved by voters to pay for technology. This approach is risky because taxpayers can be saddled with debt that outlives the devices by many years. In addition, it gives the appearance that device purchases are one-time expenses rather than recurring ones. Some have suggested using bonds with shorter lengths, closer to the expected life expectancy of the devices. In Ann Arbor, MI voters passed a 5-year technology bond. School leaders should carefully evaluate the benefits of bonds because many devices can be more cheaply replaced than repaired in just a few years.[48] In California, a new type of school bond was introduced to provide school districts with an ongoing funding source for education technology that also protects taxpayers from incurring long-term debt.[49] Contact local government agencies to determine what additional funding options are available for technology purchases.

In addition to identifying funding sources, school and district leaders should consider how cost savings in other areas could offset technology investments. For example, funds typically

dedicated to textbooks, printed materials, or other instructional resources may be redirected to devices that make such resources obsolete. Several districts, including Huntsville, AL[50] and Mooresville, NC[51] have stopped purchasing textbooks, allowing for the redistribution of funds to support digital learning.

Saving Money with Open Educational Resources

An increasing number of schools and districts are transitioning to Open Educational Resources (OER), also known as openly licensed educational resources, to reduce content licensing costs. OER are teaching, learning, and research resources that reside in the public domain or have been released under a license that permits their free use, reuse, modification, and sharing with others. OER can include complete online courses, modular digital textbooks as well as more granular resources such as images, videos, and assessment items. In addition to the potential long-term savings from the elimination of licensing fees, open resources may have the added benefit of allowing teachers to customize and share their materials with others without violating licensing agreements. The U.S. Department of Education's #GoOpen initiative works with states, school districts and educators using openly licensed educational materials to transform teaching and learning. For more information about #GoOpen visit https://tech.ed.gov/open.

Setting a Refresh Cycle

As a best practice, schools and districts should set a standard refresh cycle for computing devices, usually between 3-5 years. To minimize environmental harm, devices should be disposed of by resale, donation, salvage, or recycling. Investigate local legal restrictions and district policies before considering resale. The Electronic Product Assessment Tool provides information about the environmental impact of technology purchases and disposal. For information on more environmentally friendly technology, consult the SmartIT paper published by the Consortium of School Networking (CoSN) at www.cosn.org/smartIT.

Account for battery replacement costs when planning device purchases. Some states, such as Maine, include battery replacement and recycling costs when calculating annual costs per student because batteries often require replacement before devices reach end of life. Battery life often declines as devices age.

Strategies for Managing Devices and Application

Mobile Device Management (MDM) consists of technical platforms and managerial policies that help maintain and monitor distributed mobile devices. MDM platforms can deploy content or software updates, remotely track or wipe stolen devices, and determine what content can be installed or accessed on the devices. MDM allows these tasks to be done from a central location instead of staff having to physically touch each device, saving time and money. Most operating systems have built-in mobile device management tools or support third-party device management tools. *See Section 5. Responsible Use, Privacy, and other Considerations - Device Management for more information.*

Warranties and Maintenance

Schools and districts should plan to minimize learning disruptions by quickly addressing device maintenance and repairs. These services can be performed by school employees or outside contractors. Some schools supplement professional technical support with student support teams.

Depending on staff expertise, repairs may need to be performed on- or off-site. Maintenance strategies should include providing students and staff with replacement or loaner devices to minimize negative learning impacts during repair windows. Before signing service contracts, determine which repair issues the school or district will handle and which will require vendor support. Warranties can cover the cost of parts and/or labor to lessen repair costs. When possible, match warranties to device refresh cycles. If outsourcing maintenance, provider service-level agreements (SLAs) should clarify responsibilities for all parties.

Some schools and districts that provide students with mobile devices use a self-insurance model to defray the cost of accidental damage. For example, Southeast Valley Schools in Iowa requires a $25 annual self-insurance fee for students who receive a school-issued laptop.[52]

Help desk systems can help IT staff track and prioritize trouble tickets submitted by users. Select a system that allows staff to pull reports that can be used to evaluate technology support demand, trends, and ticket time-to-resolution (TTR).

STUDENTS AS TECH SUPPORT

At Burlington High School in Burlington, MA, 10-12th grade students enrolled in the semester-long Student Technology Innovation and Integration course provide many technology help desk services. This elective class, worth up to 2.5 credits toward graduation, began in 2011 when the school implemented a 1:1 program but lacked funding to hire additional technology support staff. Students must apply and go through an interview process to be accepted in the course and can enroll for up to 2 full years (4 semesters). In addition to providing basic tech support services, help desk students have created a Burlington High School Help Desk website where students blog, create technology resource guides for students and teachers, and write educational app reviews. Students also host a YouTube channel, BHS Help Desk Live, that features video interviews on education technology related topics. The course also includes a strong digital citizenship component, as students learn how to leverage social media to create a positive digital footprint. The Help Desk program was so successful that it has been extended to Marshall Simonds Middle School and Fox Hill Elementary School.

District Devices at Home

Districts that send devices home with students should develop policies that clarify expectations pertaining to acceptable use and lost or damaged devices. These policy considerations and others are addressed in Section 5. Responsible Use, Privacy, and Other Considerations.

Know Students' Home Internet Access

It is important for schools and districts to consider the needs of students without home Internet access. Even if students are allowed to take devices home, those without home access may struggle to complete homework assignments. Some families may not be able to afford home Internet access, or they may live in a rural area where home connectivity is not available. Other students may have home Internet access, but still have difficulty completing homework because they share a single computer with multiple family members. Schools and districts need to plan carefully to ensure that technology implementations do not exacerbate existing inequities.

There is no "one-size-fits-all" solution for these challenges. Some schools and districts use devices and/or web applications that allow students to work offline. Some provide wireless access on school buses or allow students to stay on campus after school to complete assignments. Others partner with local businesses, libraries, YMCAs, or community centers to provide students with Internet access after school. Some schools and districts provide wireless hotspots available for students in need or partner with community organizations to provide devices.

While there is no single answer to bridging the digital divide, several organizations are working to find creative solutions. Many ISPs offer Internet packages for low-income families that cost about $10/month. The non-profit organization EveryoneOn serves as a clearinghouse for this information, allowing users to search for low-cost internet, affordable computers, and digital literacy training on their website based on their zip code. Organizations such as PCs for People refurbish recycled computers and provide affordable technology to low-income individuals and families. The U.S. Department of Housing and Urban Development's (HUD) ConnectHome program connects children and families in HUD-assisted housing with access to high-speed Internet. In addition, an increasing number of libraries are making free Wi-Fi hotspots available for checkout by community residents. CoSN's Digital Equity Action Agenda initiative includes a free toolkit with recommended actions and examples of schools and districts working to address digital equity challenges.

A COMMUNITY APPROACH TO ADDRESS THE DIGITAL DIVIDE

Recognizing that the challenges of digital equity and home Internet access are a community problem, and not just a school problem, Charlotte-Mecklenburg Schools (CMS) in North Carolina formed a community-wide Digital Inclusion Steering Team in 2014. Comprised of representatives from cross-functional community organizations including the City of Charlotte, Mecklenburg County, the Charlotte-Mecklenburg Library, the Knight School at Queens University, the Knight Foundation, and the Urban League, the group began a dialogue about ways to address digital inequities in their city. Recognizing that connectivity and device access were not enough, they formed Digital Charlotte, a collaboration dedicated to raising the digital media literacy rate of the greater Charlotte area. The organization hired a project manager to prioritize digital equity as part of the community's agenda for equitable access for all.

To help address the challenge of students who lacked home Internet access, CMS schools and Charlotte-Mecklenburg Library built a collaborative program called ONE Access, which allows Charlotte-Mecklenburg students to check out books and digital resources and access library databases by using their student identification numbers. In August 2016, the library supported CMS students by piloting a Wi-Fi lending program. Partnering with Sprint, the five libraries nearest the five highest poverty high schools allowed students to check out—for free—one of 150 available wireless hotspots for Internet access, just like they would check out a book. They also worked with the non-profit organization EveryoneOn and

community groups, including PTAs and YMCAs, to educate families about low-cost home Internet options available in their community.

CMS Schools also partner with Eliminate the Digital Divide (E2D), a local non-profit started by a CMS middle school student, Franny Miller, and her family. E2D teaches high school students to refurbish donated laptops and is narrowing the digital divide by equipping economically disadvantaged CMS students and families with at-home access to computers, digital broadband, and the digital literacy training necessary to support academic and professional success. The organization has assisted more than 2,500 Charlotte-Mecklenburg area families with technology to reduce the digital divide.

According to a recent CoSN survey, 42 percent of district technology leaders rank addressing digital equity/lack of broadband outside-of-school as a very high priority.[53] Some districts are choosing to provide students with mobile hotspots. For example, Beekmantown Central School District in West Chazy, NY offers free mobile hotspots to students who do not have Internet at home, with both the device and the monthly service fee paid for by the district via the Extended Learning Time Grant.[54] Other districts partner with local libraries that make mobile hotspots available for checkout. Students who do not have Internet or a device at home at Indian Trail High School and Academy just south of Milwaukee, WI can go to the school library to check out a laptop and a mobile hotspot to complete homework with just like they would a library book.[55]

BRIDGING THE HOMEWORK GAP BY PROVIDING FILTERED WI-FI HOTSPOTS

Recognizing the important role that home Internet access plays with the advent of "everywhere, all-the-time" learning, Green Bay Area Public Schools in Wisconsin now allows students in grades 1-12 to check out Wi-Fi hotspots and laptops from school libraries for up to three consecutive days. The program is designed to help reduce the negative educational impact for students without home connectivity as teachers increase the use of technology in instruction.

Looking for a managed mobile broadband solution with vendor-provided content filtering, district leaders settled on an initial pilot of 100 mobile hotspots. Before deployment, district technology staff tested the devices at locations across the city to be sure that cellular coverage was available in the communities of greatest need. Classroom teachers in the 10 secondary schools piloting the program identified students lacking home Internet access and/or computing devices and nominated them for checkout privileges. One unforeseen challenge was the social stigma of poverty initially associated with the program. To prevent these negative associations, students currently check out the devices using an unmarked computer bag.

As demand for the hotspots grew, district leaders expanded the number of hotspots to 350 in 2015-2016 and, as of May 2017, now have loaner hotspots available in all Green Bay Area public schools. To sustain the momentum, next steps include training teachers and library media specialists to better support students with device check out, engaging the parent community about the checkout option, and providing ongoing device maintenance.

When considering whether to allow students to take district-provided devices home during the school year, anticipate family and student interest in taking devices home over the summer. Some schools launching 1:1 programs delay the summer option for a year or two so they better understand and meet repair needs. Others do not allow students to take devices home over the summer.

DETERMINING STUDENT ACCESS AT HOME

Fairfax County Public Schools in northern Virginia includes home access questions on emergency information forms that are updated annually. Families are asked if they have home Internet access and if they have adequate devices at home for students to do homework. The question about devices was added because even if there is a computer in the home, it may be shared by multiple children and adults and thus may not always be available for students to do homework. The district-wide survey is initially sent out via email and followed up with an automated telephone survey to home and cell phones. Schools then make individual phone calls and send home paper surveys in backpacks to families who have still not responded. "It may seem obvious, but surveys that are only email or web-based will likely miss the families you are most concerned about," notes Fairfax's CTO. In addition, recognizing that not all parents and guardians are fluent in English, Fairfax issues all surveys (web, phone, paper) in multiple languages. The district includes the survey information as required fields in their student information system (SIS), making the information easily accessible to teachers and school officials.

Choosing a Rollout Model

Four possible models for device rollout are outlined here, each of which can be used in conjunction with the others. The best rollout model is one that meets the needs and capacities of the school or district deploying the devices. Regardless of the model selected, consider piloting it first to allow for necessary adjustments before deploying devices at scale.

Full school: The entire student body of a school receives devices at the same time.

Pros: Creates a cultural shift towards digital learning within the school. High school rollouts can benefit from wholesale 9–12 deployment because multi-grade classrooms in high school may make grade-by-grade implementation difficult.

Cons: Provides limited opportunity to work out the kinks at the school level. Professional development and logistics must be carefully planned.

Grade level: Over the course of several years or throughout a single year, distribute devices to students one grade level at a time. With this model, educational goals and teacher readiness often drive which grades are selected. When devices are distributed starting with the lowest grade in a school, students take the devices with them as the age up. This may work best for middle and elementary schools due to the difficulties presented by multi-grade classrooms in high school as identified above.

Pros: Schools and districts deploy fewer devices to start, providing opportunities to work out unanticipated challenges on a smaller scale. Grade-level implementations may encourage teachers to collaborate more closely with their same-grade colleagues.

Cons: Runs the risk of losing funding for the next grade level and creates inequity of access across grade levels.

Subject area: Devices are rolled out to a focused discipline or content areas within schools. This is effective if a school has a discipline focus, such as STEM or the arts, that will be enhanced with this device model. Consider choosing subjects for which there is already community buy-in regarding the potential for technology to improve instruction.

Pros: Allows an additional focus on the educational requirements of a specific subject. Less expensive than a school wide rollout and allows time for lessons learned (similar to a grade-level rollout).

Cons: The student experience may be uneven across classrooms, teachers, and/or subject areas. Some teachers may lack interest or ownership in using devices for learning because they see them as belonging to other programs or subject areas. Other teachers may want to use the technology to support their subjects as well.

Exemplar teacher model: Work first with the teachers who can and are interested in helping build a program. Outline the digital learning vision and exemplar teacher participation requirements. Have interested teachers apply for consideration and submit examples of their work that align with district plans.

Pros: Works through the process with power users and early adopters to develop policies, protocols, and procedures. There is a greater chance of initial success that can help build momentum. Allows for adjustments from lessons learned.

Cons: Non-pilot teachers may feel disconnected from the process. Could also result in policies and professional development strategies that fail to take reluctant users into account.

FULL-SCHOOL PILOT MODEL

When the Houston School District kicked off its 1:1 laptop PowerUp initiative, the district ramped up the initiative in phases throughout the school year so that infrastructure capacity could be tested and adjusted. It used a full-school pilot model for the initial rollout. At the start of the pilot, teachers at 11 high schools received laptops. Six months later, all students in the pilot high schools received laptops. The program ultimately expanded to provide 130,000 students in grades 3–12 with laptops. Before implementing the program, the district superintendent and CTO observed several other 1:1 programs to learn from them and to brainstorm improvements.

Planning Device Rollouts

Careful planning is required to ensure smooth device rollouts. Schools and districts need to develop plans unique to their needs and context. Within a district, individual schools will most likely need some leeway in developing processes that best suit their school populations.

Schools and districts should determine in advance how to track the influx of devices associated with 1:1 device deployments. Many schools and districts leverage existing capacity and systems by using existing inventory systems, such as those used in libraries or media centers. Others use more specialized technology inventory systems.

Consider parents as partners in this process, especially if providing devices for home use. Plan informational meetings before distributing devices to address parent concerns and walk them through policies and procedures. Take into account the availability of the parent population

when scheduling these events so as to meet face-to-face with as many parents as possible. Some schools make parent meetings mandatory while others video record the sessions for parents who cannot attend. Base parent information sessions on the needs of individual school communities and supplement these sessions with other communications tools such as parent newsletters, training opportunities, student-led technology nights, blogs, and social media. Keep the lines of communication open.

Parents and other community members should be kept informed during the entire digital transition process. Providing as much advance information as possible demonstrates that the initiative is being launched with a clear vision and plan.

Ongoing professional development on the most effective use of digital learning resources should begin before teachers receive devices and continue throughout the school year. Consider planning an introductory course (online, in person, or blended) to help teachers learn basic device functionality and troubleshooting in advance. The same course could be modified for students to ensure a shared foundation of understanding before the rollout.

While some students will be adept at device usage from the moment they receive one, others will need guidance, and all will require help accessing new digital learning resources. Consider preloading devices with an electronic handbook that explains account and sign-on procedures.

COMMUNICATING WITH STAKEHOLDERS

Before implementing its 1:1 initiative, the St. Vrain Valley School District in Colorado formed an instructional technology advisory committee to plan the district's transition to digital learning. Throughout the technology planning and implementation process, the district's goal was to communicate often, build trust with the community through transparency, and maintain the focus on learning. To keep lines of communication open, the district created a blog to communicate its story and give stakeholders an opportunity to provide feedback.

The technology department placed a shortcut on the home screen of every device to provide families with information and resources about the transition. The shortcut included information in both English and Spanish as 20 percent of the population is Spanish speaking. In addition, the district reached out to community groups working with local families and partnered with libraries and businesses to provide family events and trainings.

St. Vrain's communication outreach has evolved over time. The district has implemented its 1:1 initiative in grades 6-12 and has provided classroom sets of tablets and computers at the elementary level. The district helped solidify the home-school connection by providing voluntary "Camp iPad for Parents" events throughout the academic year with the goal of engaging, empowering, and informing parents in how the devices can enhance their child's learning opportunities. The district also created a monthly family connections newsletter to provide families with ongoing information and support.

5. Responsible Use, Privacy, and Other Considerations

IN THIS SECTION

- Device management
- Responsible use and digital citizenship
- Student privacy requirements
- Safeguarding against inappropriate content
- Policies for lost or damaged devices

Before deploying devices, schools and districts should set policies and communicate expectations regarding topics such as device management, responsible use, digital citizenship, safeguarding student privacy, and managing lost or stolen devices. These considerations are essential to ensure the success of educational technology initiatives.

Device Management

REMOTE MANAGEMENT

Computing devices require ongoing management, which can include installing software updates, adjusting content filter settings, and modifying system preferences. Keeping security and privacy settings up to date can prevent malware and help protect student data. There are a variety of software tools that can provide centralized software updates. Schools using online assessments may need to install specific software to ensure secure testing environments.

Because some management tools may collect location information and/or data about how devices are used, it is important to address privacy concerns by clearly communicating remote device management policies to students and families. Internally, schools and districts should clearly outline employee policies and procedures regarding device monitoring to prevent potential abuse.

REMOTE THEFT PROTECTION

Schools and districts may consider installing tools that can remotely disable or erase devices in the event of loss or theft. Adding a sticker on the bottom of each device stating that it can be remotely disabled may serve as a theft deterrent. In addition, consider engraving the devices with the school name or logo to make it more difficult for stolen devices to be re-sold. This can

improve the odds that lost devices are returned and help prevent the loss of confidential data. Local law enforcement agencies may be good resources for determining how best to deter theft and address missing devices.

STUDENT ACCESS

Schools and districts need to decide how much control students may have over school-provided devices. Locking down devices improves security and makes it easier for IT staff to maintain them, but gives students less freedom to personalize devices for their needs. Policies allowing tiered levels of device control may be used to provide students who demonstrate responsible behavior more privileges while restricting access for others.

Encouraging Responsible Use

Before allowing students Internet access via a school device or network, most schools ask parents and students to sign an Acceptable Use Policy (AUP) or a Responsible Use Policy (RUP). An AUP is a written agreement between parents, students, and school personnel that outlines the terms of responsible device use and consequences for misuse. AUPs traditionally cover topics such as ethical technology use, standards for student behavior and interaction, and outline websites or platforms that should not be used while on campus or using a school-provided device. Students agree to follow rules governing their Internet use and online conduct and parents acknowledge that their child agrees to the guidelines.

Schools and districts should write AUPs in plain language that is easily understood by students, parents, and district personnel. One helpful approach is to tailor AUP language to different student grade levels, as Boston Public Schools in Massachusetts has done. Involving students in AUP development can turn the process into a valuable learning opportunity and improve student buy-in. For additional information on questions to consider when drafting an AUP, see CoSN's Rethinking Acceptable Use Policies to Enable Learning: A Guide for School Districts and Common Sense Education's 1 to 1 Essentials: Acceptable Use Policies.

TEACHING DIGITAL CITIZENSHIP

Digital citizenship is defined as the safe, ethical, responsible, and informed use of technology. This concept encompasses a range of skills and literacies that can include Internet safety, privacy and security, cyberbullying, online reputation management, communication skills, information literacy, and creative credit and copyright. Increased connectivity increases the importance of teaching learners how to become responsible digital citizens.

Educators need to guide the development of these competencies so students learn how to use technology in ways that are meaningful, productive, respectful, and safe. For example, helping students learn proper online etiquette, how their personal information may be collected and used online, and how to leverage access to a global community to improve the world around them can help prepare them for successfully navigating life in a connected world. Mastering these skills requires a basic understanding of the technology tools and the ability to make increasingly sound judgments about the use of them in learning and daily life. For the development of digital citizenship, educators can turn to resources such as Common Sense Education's digital citizenship curriculum or the student technology standards from the International Society for Technology in Education (ISTE). Additional information about cyberbullying prevention can be found at StopBullying.Gov and from the Readiness and Emergency Management for Schools Technical Assistance Center.

Effective AUPs help teach students to create a positive digital persona. Learning responsible digital citizenship while in school helps students to thrive in a connected world. Digital citizenship education can range from online etiquette and safety to privacy awareness and cyberbullying prevention. Provide families with guidance to help them establish their own acceptable use norms at home. Many districts hold a mandatory parent orientation before issuing devices to students and coordinate with parent organizations to lead classes on technology use in the home. Hosting parent and community nights to educate parents about the school's approach to connected learning, security and privacy policies, and digital citizenship helps families share the responsibility for encouraging appropriate use.

Protecting Privacy

Schools officials, families, and software developers must be mindful of how data privacy, confidentiality, and security practices affect students. Schools and districts have an obligation to tell students and parents what kind of student data the school or third parties (e.g., online educational service providers) are collecting and how the data can be used. Develop policies that identify who has access to student data and clearly communicate to families their rights and responsibilities concerning data collection. These policies should include both formal adoption processes for online educational services and click-wrap agreements. Click-wrap agreements appear when users are asked to accept the provider's terms of service before using a website or software application. Click-wrap agreements enter the developer and the user (in this case, the school or district) into a contractual relationship akin to signing a contract. Ensure district employees understand the implications of district policies governing the use of such software agreements.

A number of statutes apply to student privacy in schools. More information on each is below.

FERPA (the **Family Educational Rights and Privacy Act**) gives parents the right to access and seek to amend their children's education records (these rights transfer to students when they reach 18 years of age or when they attend a postsecondary school at any age). FERPA protects personally identifiable information (PII) in students' education records from unauthorized disclosure, and requires prior written consent before schools disclose PII from student education records. However, one exception to FERPA's general consent requirement permits a school to disclose PII from students' education records to a third party to whom the school has outsourced institutional services or functions, as long as certain conditions are met. Under this exception, the outside party must perform an institutional service or function for which the educational agency or institution would otherwise use school employees, the outside party must be under the direct control of the educational agency or institution with respect to the use and maintenance of education records, and the third party must be subject to the FERPA requirements governing the use and disclosure of PII from education records found in 34 CFR § 99.33(a). For more guidance on FERPA, visit the US Department of Education's FERPA resources.

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

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

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

PPRA (the **Protection of Pupil Rights Amendment)** is intended to protect the rights of parents and students in two ways. First, PPRA seeks to ensure that schools and contractors make instructional materials available for parents' inspection if those materials will be used in connection with a survey, analysis, or evaluation funded by the U.S. Department of Education. Second, PPRA requires that a school district, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from the students for marketing purposes or for sale or provision to others for marketing purposes and give parents the opportunity to opt out of these activities. One important exception to PPRA is that neither parental notice and the opportunity to opt out nor the development and adoption of policies are required for school districts to use students' personal information for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools.

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

Consult PTAC Recommendations

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a one-stop resource to learn about privacy related to student data. PTAC provides information and updated guidance on privacy, confidentiality, and security practices through a variety of means, including training materials and direct assistance. PTAC also provides guidance on the relevant privacy laws. PTAC recently provided additional recommendations on Protecting Student Privacy while Using Online Educational Services and Transparency Best Practices for Schools and Districts.

SHARE DATA WISELY

As a general rule, if a school provides a device, has an educational service contract with a vendor performing an institutional function or service, and the application has educational value, then collecting data for purposes of helping the student or teacher or to improve the application itself is generally permitted. However, per the requirements of FERPA's "school official" exception, data uses must be authorized by the school and constitute a legitimate educational interest per the school's annual notification of FERPA rights. For districts that rely on the general terms of service (TOS) offered by outside providers, PTAC provides additional guidance.

Safeguarding Against Inappropriate Content

Schools have a responsibility to protect students from inappropriate Internet content when using school-provided devices or networks. This can be done using technical approaches such as content filtering as well as through the implementation of a digital citizenship curriculum.

TECHNICAL CONTENT FILTERING

Many tools are available to filter web-based content and schools and districts that receive E-Rate funds are required to do so. Schools must balance protecting students from inappropriate content with providing access to high quality educational resources. Overly strict filtering can interfere with educational goals. For example, filters that block broad content categories like gaming or social media without exception can also block educational games and collaboration tools.

Content filtering should be managed as a partnership between teachers, students, and technical staff. There should be a streamlined and well-communicated process for teachers to request that educationally valuable sites be unblocked. When requests cannot be accommodated, it is important for technical staff to clearly communicate the reason why. Content filtering protocols should be periodically audited to make any necessary adjustments.

While technical filtering tools should always be in place, teaching students to be responsible Internet users is the best long-term strategy. No technical filtering tool is 100 percent reliable. Some objectionable content may still pass through, and savvy students will often find ways to circumvent filtering solutions. In addition, because students will use devices without content filtering such as home computers or personal smartphones, they need to learn how to exercise good judgment and navigate the Internet safely. For this reason, implementing a robust digital citizenship curriculum is essential to keep students safe online.

INFORMING PARENTS

In general, schools are not required to provide content filtering when a device is not used on a school-provided network. It is a good practice, however, to provide filtering on school-owned devices even when they are used off campus. Clearly communicate to parents when and where schools are providing filtering and provide families with guidance on home filtering options and digital citizenship education. For more information on consumer device filtering, see the FCC guide on Protecting Children from Objectionable Content.

Dealing with Lost or Damaged Devices

Districts should have a plan to address the inevitable issue of lost, stolen, or damaged devices and ensure that parents and students are aware of their responsibilities.

PREVENTING DEVICE DAMAGE OR LOSS

The best way to deal with device loss or damage is to prevent it from happening in the first place. The following suggestions can help prevent and reduce rates of device damage and loss:

Teach students responsible practices. Talk with students about how to best protect their devices. These conversations can range from how to safely carry a laptop across a classroom to theft prevention.

Allow students to customize their devices. Students have a greater sense of ownership when allowed to customize their devices. Customization may include putting stickers on the device and choosing a unique (but school-appropriate) desktop background image. Customization also makes it easier for students to identify their devices.

Require password protection. Password protect student devices and implement policies that require students to re-enter passwords when their device has not been use for a predetermined period of time. This can make devices less attractive to thieves and protect student privacy.

Provide sturdy carrying cases for devices. Many mobile devices are broken by students dropping a heavy backpack with a mobile device inside. A well-padded laptop bag or carrying case can help protect devices from accidental damage.

Use mobile device management software to locate a missing device and remotely render it inoperable. If a device is lost or stolen, mobile device management software can help schools and districts alert authorities to the location for retrieval. Establish clear policies that limit the use of location monitoring to emergency situations or when the device has been reported lost or stolen. Clearly communicate these policies to stakeholders to address potential privacy concerns.

DEVICE PROTECTION AT ALL GRADE LEVELS

Even the youngest learners can be taught how to protect their devices. A kindergarten teacher at Pachappa Elementary School in Riverside Unified School District in Riverside, CA shared her strategy for teaching her students how to care and protect their devices. Each kindergartener uses a small plastic tub (the kind designed for leftovers) to store his or her device when not in use. The teacher tells the students, "That's their device's 'house.'" The plastic case that originally packaged the device is its "bed." Kindergartners are taught to tuck their device into bed, wrapped in a cloth, its "blanket." Then they put a "seat belt" (a rubber band) around the case so that it will not "fall out of bed." Children carry their device's "house" between school and home in their backpacks.

DEALING WITH DEVICE DAMAGE OR LOSS

Whatever the strategy for dealing with lost or stolen devices, make sure it is clearly communicated to families and students. Some strategies used by districts include:

Require payment. Some districts require the student or family to pay for a device that is missing or damaged. The advantage to this approach is that it holds users accountable but it can pose challenges for families unable to afford the cost of repair or device replacement. Schools and districts choosing this route should provide options for reduced or installment payments.

Contract insurance. Insurance policies are the simplest way to handle lost or missing devices, but are potentially more expensive. The insurance policies can be paid for either by the district or by families. If the latter, the district may need to have a solution in place for families who cannot afford the cost of device insurance. Consider a reduced rate or installment plan for these families.

Self-insurance. Some districts may charge a self-insurance fee to cover the cost of missing or damaged devices. These funds are set aside to repair or replace devices as needed. With this approach there is a risk that repair and replacement costs might exceed the self-insurance funds, but this can be a less expensive solution than contract insurance.

Maintain extra inventory. To minimize the negative impact on learning, it is always a good idea to have "hot spares" available to temporarily replace devices that are lost or damaged.

Schools and districts may establish policies that allow students to "earn" additional device-related permissions after proving themselves responsible caretakers. For instance, students may be allowed to customize their desktop or home screen or take the device home over the summer. Similarly, students who damage or repeatedly lose their device might lose these privileges or be given an older or less expensive device. These decisions should balance accountability with the need to provide the student with the necessary tools for schoolwork.

Conclusion

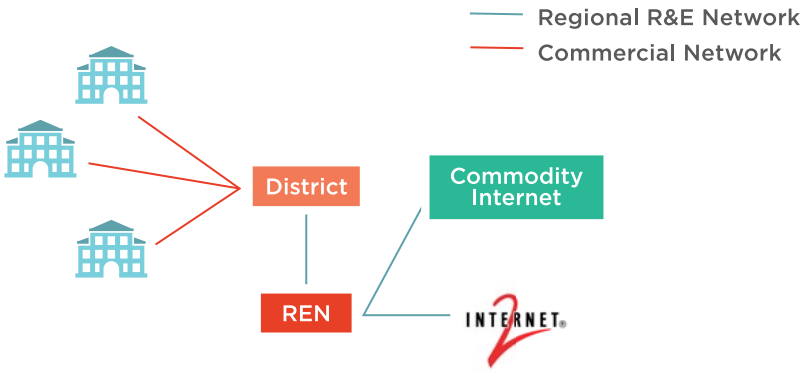
An essential element of providing equitable education for America's students is ensuring the existence of technology infrastructure to support personalized learning, high-quality instruction, collaboration, increased engagement, and creativity. Planning and providing infrastructure, both Internet connectivity and devices, should stem from a clear vision for how learning and teaching will be supported. This involves understanding a variety of technical options and legal requirements as well as seeking input from teachers, leaders, students, parents, and community members.

Our students live in a connected world where they will be expected to engage and interact with peers and experts online, create and design with digital tools, and be exemplary digital citizens. With vision, infrastructure, professional learning, and devices, our schools will be better able to support students with the opportunity to learn and thrive.

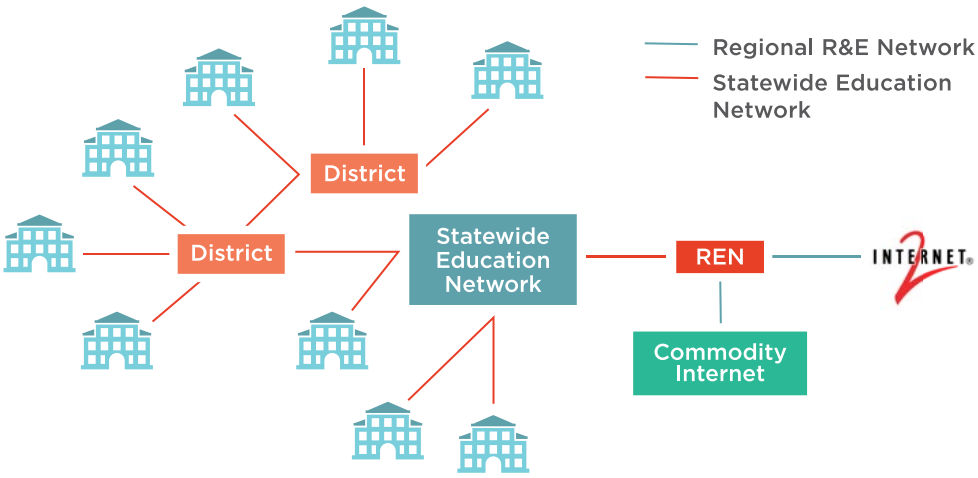
Appendix A

REN Connection Paths

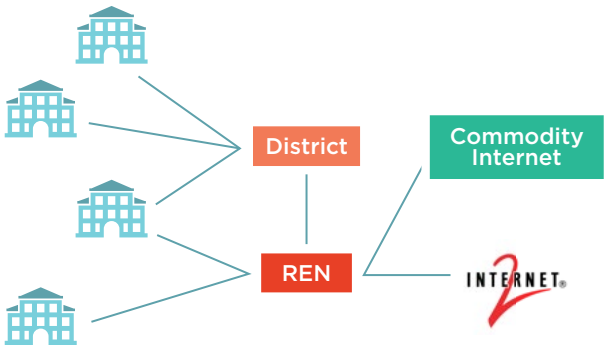
1. District connects to the REN and commercial network operators provide last mile connectivity to schools.



2. A Statewide Education Network connects K-12 schools and/or districts to REN.



3. K-12 schools and/or district connect directly to the REN.



Appendix B

Quick Reference Guide: Key Questions

This list identifies many important questions to consider before implementing digital learning initiatives. Each set corresponds to further guidance within this Guide.

1. Getting Started: Assess the Current Situation and Set Future Goals (see Section 1)

- What is the vision for learning that technology will be supporting?
- What digital learning resources will be needed?
- What kind of professional development will teachers need to facilitate digital learning?
- What is the current state of the organization's physical infrastructure?
- How many and what types of devices does the existing network support? What is planned for the future?
- What resources are available to fund the transition?

2. Getting High-Speed Internet to Schools (see Section 2)

- What are the options for high-speed Internet access in the area?
- What is the best connectivity path for the school or district?
- What local factors will affect connectivity costs?
- What funding sources are available?
- What resources are available for schools in rural communities?

3. Getting High-Speed Internet Throughout Schools (see Section 3)

- What are the necessary steps for planning school wireless network?
- What physical infrastructure considerations will impact the network?
- How should the network be provisioned, configured, and managed?
- How should security risks to the network be managed?

4. Getting Devices to Students and Teachers (see Section 4)

- Which factors should be considered in device selection?
- Is a BYOD program a potential option?
- If so, how will the school or district address the needs of students without devices or home Internet connectivity?
- What funding sources are available to pay for devices?
- How frequently will devices be updated or refreshed?
- How will devices be maintained?
- Should students be allowed to take school-provided devices home?
- How should devices be rolled out?

5. Determining Responsible Use, Student Privacy, and Other School Policies (see Section 5)

- How should devices be managed?
- How can schools ensure and encourage the responsible use of devices?
- What are school obligations for protecting the privacy of students?
- How should devices be filtered?
- Which policies for lost or damaged devices make sense?

References

[1] Consortium for School Networking (CoSN). *2014 Annual E-Rate and Infrastructure Survey.* 2014. Web. http://cosn.org/sites/default/files/pdf/CoSN%202nd%20Annual%20E-rate%20and%20Infrastructure%20Report,%2010-15-2014_2.pdf

[2] Consortium for School Networking (CoSN). *2016 Annual Infrastructure Survey.* 2016. Web. http://www.cosn.org/sites/default/files/CoSN_4th_Annual_Survey_Nov%202%20FINAL.pdf

[3] U.S. Department of Education, Office of Educational Technology, Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update, Washington, D.C., 2017. https://tech.ed.gov/netp.

[4] Consortium for School Networking (CoSN). *2016 Annual Infrastructure Survey.* 2016. Web. http://www.cosn.org/sites/default/files/CoSN_4th_Annual_Survey_Nov%202%20FINAL.pdf

[5] Ibid.

[6] "2016 State of the States Report." Education Superhighway, 17 Jan. 2017. Web. https://s3-us-west-1.amazonaws.com/esh-sots-pdfs/2016_national_report_K12_broadband.pdf

[7] National Telecommunications and Administration Association and National Science Foundation. "National Broadband Research Agenda." National Telecommunications and Administration Association, Jan. 2017. Web. https://www.ntia.doc.gov/files/ntia/publications/nationalbroadbandresearchagenda-jan2017.pdf.

[8] "2015 Broadband Progress Report." Federal Communications Commission. N.p., 28 Jan. 2016. Web. https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-10A1.pdf

[9] "Types of Broadband Connections." Federal Communications Commission, 24 June 2014. Web. https://www.fcc.gov/general/types-broadband-connections.

[10] "Summary of the E-Rate Modernization Order." Federal Communications Commission. N.p., 08 Oct. 2015. Web. https://www.fcc.gov/general/summary-e-rate-modernization-order

[11] "2016 State of the States Report." *Education Superhighway,* 17 Jan. 2017. Web. https://s3-us-west-1.amazonaws.com/esh-sots-pdfs/2016_national_report_K12_broadband.pdf

[12] Ibid.

[13] Fox, C., Jones, R. (2016). The Broadband Imperative II: Equitable Access for Learning. Washington, DC: State Educational Technology Directors Association (SETDA). http://www.setda.org/wp-content/uploads/2016/09/SETDA-Broadband-ImperativeII-Full-Document-Sept-8-2016.pdf

[14] Ibid.

[15] U.S. Department of Education, Office of Educational Technology, Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update, Washington, D.C., 2017. https://tech.ed.gov/netp

[16] Consortium for School Networking (CoSN). *Rethinking Educational Equity in a Digital Era.* 2014. Web. http://www.cosn.org/sites/default/files/pdf/Rethinking%20Educational%20Equity%20in%20a%20Digital%20Era,%20June%202014.pdf.

[17] Donohue, N. "A Working Model for Blended Learning in an Urban School." *Edutopia.* GEORGE LUCAS EDUCATIONAL FOUNDATION, 07 July 2014. Web. https://www.edutopia.org/blog/working-model-for-blended-learning-nicholas-donohue-lourenco-garcia

[18] Fox, C., Jones, R. (2016). The Broadband Imperative II: Equitable Access for Learning. Washington, DC: State Educational Technology Directors Association (SETDA). http://www.setda.org/wp-content/uploads/2016/09/SETDA-Broadband-ImperativeII-Full-Document-Sept-8-2016.pdf

[19] Acree, L., Fox, C (2015). State Digital Learning Exemplars. Raleigh, NC. Friday Institute for Educational Innovation at the NC State University College of Education and the State Educational Technology Directors Association. http://www.setda.org/wp-content/uploads/2015/10/DigitalLearningExemplars_June2015.pdf

[20] "EXECUTIVE ORDER S-21-06." Office of Governor Edmund J. Brown, n.d. Web. https://www.gov.ca.gov/news.php?id=4818

[21] CTC Technology and Energy. "Dark Fiber Lease Considerations." 2012. Web. http://www.ctcnet.us/DarkFiberLease.pdf

[22] Gonzales, L. "Dark Fiber Paying Off in Florida's Lakeland." Community Networks, 1 Aug. 2013. Web. https://ilsr.org/dark-fiber-paying-off-in-floridas-lakeland/

[23] Thompson, J. Ryan, David Talbot, and Keith Krueger. (2016) Maximizing K-12 Fiber Connectivity Through E-Rate: An Overview. CoSN. Web. http://www.cosn.org/sites/default/files/CoSN-ERATE-toolkit-Revised17Apr2016.pdf

[24] Erlanger, Leon. "Fiber: The Connectivity Solution Schools Need." Edtech Magazine, 12 Apr. 2017. Web. http://www.edtechmagazine.com/k12/article/2017/04/fiber-connectivity-solution-schools-need.

[25] Herold, Benjamin. "Districts Get Creative to Build Faster Internet Connections." Education Week. 14 Jan. 2014. Web. http://www.edweek.org/ew/articles/2014/01/15/17fiber_ep.h33.html

[26] Birkenbuel, Renata. "Butte Schools' Fiber Optics Switch Featured in Nationwide Magazine." Montana Standard. Montana Standard, 21 Jan. 2014. Web. http://mtstandard.com/news/local/butte-schools-fiber-optics-switch-featured-in-nationwide-magazine/article_d2cba792-826a-11e3-a083-001a4bcf887a.html.

[27] "Types of Broadband Connections." Federal Communications Commission, https://www.fcc.gov/general/types-broadband-connections#wireless. Web.

[28] The Utah Education Network (2012). Welcome to UEN. Retrieved from http://leadershipsummit.setda.org/wp-content/uploads/sites/5/2013/11/Welcome-to-UEN.pdf.

[29] "UEN Info." (n.d.): n. pag. Utah Education Network. Web. Retrieved from http://www.uen.org/ueninfo/downloads/booklet.pdf.
[30] "Schools and Libraries (E-Rate)." School and Library Eligibility - Schools and Libraries Program - USAC.org. Universal Service Administrative Company, n.d. Web. http://www.usac.org/sl/applicants/beforeyoubegin/definitions.aspx.
[31] "Summary of the E-Rate Modernization Order." Federal Communications Commission, 08 Oct. 2015. Web. https://www.fcc.gov/general/summary-e-rate-modernization-order.
[32] Navajo Nation Telecommunications Regulatory Commission. (2013). FCC Modernizing the E-Rate Program for Schools and Libraries: Comment from The Navajo Nation Telecommunications Regulatory Commission. Available at http://apps.fcc.gov/ecfs/document/view?id=7520944058
[33] Consortium for School Networking (CoSN). *2016 Annual Infrastructure Survey.* 2016. Web. http://cosn.org/sites/default/files/CoSN_4th_Annual_Survey_Oct16_PROOF5.pdf
[34] Jones, R. & Fox, C. (2016). State K-12 Broadband Leadership: Driving Connectivity and Access. Washington, DC: State Educational Technology Directors Association (SETDA)
[35] "Bridging the Digital Divide for Low-Income Students." Digital Promise, 7 Apr. 2016. Web. http://digitalpromise.org/2014/04/07/11-learning-24-7-at-sunnyside-unified-school-district/
[36] Ibid.
[37] Native American Advancement Foundation, n.d. Web. https://www.naafnow.org/after-school.
[38] "Overview of the Gigabit Ethernet Standard." SearchNetworking. N.p., n.d. Web. http://searchnetworking.techtarget.com/tutorial/Gigabit-Ethernet-standard-Overview-of-1000BASE-Ethernet-lesson-5b.
[39] Consortium for School Networking (CoSN). *2016 Annual Infrastructure Survey.* 2016. Web. http://www.cosn.org/sites/default/files/CoSN_4th_Annual_Survey_Nov%202%20FINAL.pdf
[40] Ibid.
[41] W-2 Phishing Scam Now Targeting Schools. Privacy Technical Assistance Center, U.S. Department of Education, Feb. 2017. Web. http://ptac.ed.gov/sites/default/files/W2%20Phishing%20Scam.pdf.
[42] Doran, Leo. "Ransomware Attacks Force School Districts to Shore Up-or Pay Up." Education Week, 08 Feb. 2017. Web. http://www.edweek.org/ew/articles/2017/01/11/ransomware-attacks-force-school-districts-to.html.
[43] Lindros, Kim, and Ed Tittel. "What Is Cyber Insurance and Why You Need It." CIO, 04 May 2016. Web. http://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html.
[44] Chariho School District. (n.d.). Chariho 1:1 - An Investment in the Future: Our Journey Toward a Vision for Technology Use. Available at http://www.chariho.k12.ri.us/sites/default/files/1-1_vision.pdf
[45] Chariho School District. (n.d.) Chariho 1:1 Device Selection Advisory Committee. Available at https://www.chariho.k12.ri.us/sites/default/files/device_selection_advisory_committee_members.pdf
[46] Lhamon, C. U.S. Department of Education, Office for Civil Rights. (2014, October 1). Dear Colleague Letter: Resource Comparability. Available at https://www2.ed.gov/about/offices/list/ocr/letters/colleague-resourcecomp-201410.pdf.
[47] The text of the ESEA, as amended by ESSA, is available at: http://legcounsel.house.gov/Comps/Elementary%20And%20Secondary%20Education%20Act%20Of%201965.pdf. See sections 4109(a)(2) and 4109(b).
[48] "2012 Technology Bond Program." Ann Arbor Public Schools, n.d. Web. http://www.a2schools.org/Page/6793
[49] Fensterwald, John. "Districts Find New Way to Fund Technology." EdSource, 7 Nov. 2014. https://edsource.org/2014/districts-find-new-way-to-fund-technology/69727.
[50] Bonvillian, Crystal. "Huntsville District Ahead in Digital Textbooks, but State Encouraging Others to Catch up (updated)." AL.com, 22 July 2012. Web. http://blog.al.com/breaking/2012/07/huntsville_district_ahead_in_d.html.
[51] Quillen, Ian. "Building the Digital District." Education Week, 29 Apr. 2016. Web. http://www.edweek.org/dd/articles/2011/10/19/01conversion.h05.html.
[52] "Chromebook Insurance Policy for Southeast Valley Schools." (N.d.): n. pag. Southeast Valley Schools. Web. http://www.southeastvalley.org/vimages/shared/vnews/stories/5772cc55def95/Chromebook%20insurance%20policy%20for%20SWG%20PV%20Schools.pdf
[53] Consortium for School Networking (CoSN). 2016 Annual Infrastructure Survey. 2016. Web. http://www.cosn.org/sites/default/files/CoSN_4th_Annual_Survey_Nov%202%20FINAL.pdf
[54] "Wireless Hotspots @ Home." Beekmantown Central School District, n.d. Web. http://www.bcsdk12.org/district.cfm?subpage=9355
[55] Barrett, Rick. "Schools Lend out Mobile Hotspots to Get All Students Online." Milwaukee-Wisconsin Journal Sentinel, 04 Apr. 2016. Web. http://archive.jsonline.com/business/schools-lend-out-mobile-hotspots-to-get-all-students-online-b99702752z1-375195281.html
[56] Straehley, D. (2013, May 24). RIVERSIDE: District introduces textbooks on iPod, other tablets. The Press-Enterprise. Available at http://www.pe.com/2013/05/24/riverside-district-introduces-textbooks-on-ipod-other-tablets/

OFFICE OF
Educational Technology

The mission of the Department of Education is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

http://tech.ed.gov