Districts Simplify BYOD with Managed Service Solution

June 2013

Sponsored By:

impulse

the JOURNAL

Table of Contents

Districts Simplify BYOD with Managed Service Solution

Many K-12 school districts are recognizing that implementing a BYOD (Bring Your Own Device) policy is an effective approach to providing their students and faculty with the opportunity to enhance the education process by leveraging 21st century technology.

However, it can represent a big cultural change for the learning environment as well as a challenge to IT professionals. How can a district implement a BYOD initiative and still maintain security and control over its computing environment? How can the District's IT Department allow personal devices on the network without adding additional technical and support resources? This whitepaper reveals how Impulse Point's Safe•Connect mobile device management (aka MDM) solution enabled BYOD initiatives at three K-12 school districts. A common thread throughout these cases is functional simplicity, real-time reporting and how a managed services approach eliminated the support burden for IT staff and enhanced the end user experience for students and faculty.

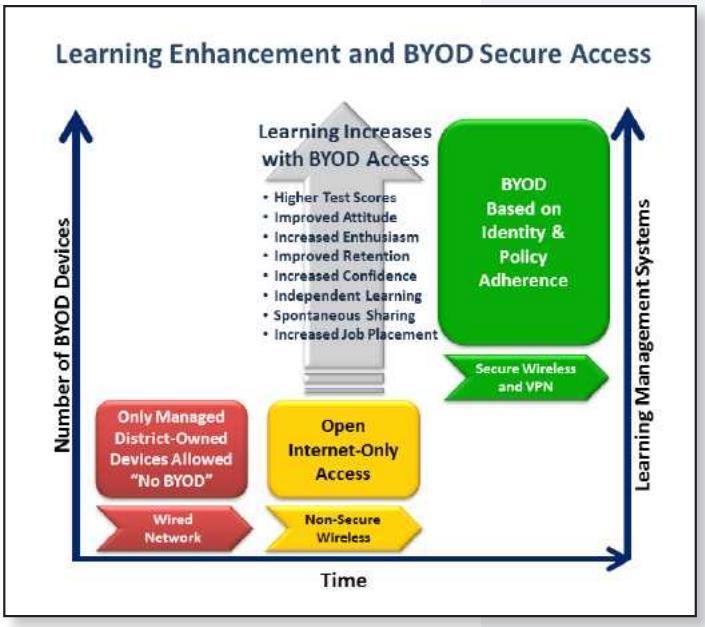
Enhancing Learning with BYOD

How can K-12 schools and districts provide students with the academic benefits of 1-to-1 computing in today's tough budget climate? Bring-your-own-device (BYOD) initiatives look like a promising answer, since students and teachers own more smartphones, tablets, and laptops than ever before.

According to a 2013 Pew Research Center survey, almost half (47 percent) of teens own smartphones up from just 23 percent in 2011. And 23 percent of teens have a tablet computer—a level comparable to the general adult population.

And more than 60 percent of parents reported that they would be willing to buy a mobile device to support learning, according to a study from Project Tomorrow, a national education nonprofit group.

Today's school districts are looking at technology as a way to improve the learning environment. According to the National School Board Association's report, *Technology's Impact on Learning*, technology-rich schools generate impressive results for students, including: improved achievement, higher test scores, better student attitude, enthusiasm, and engagement, richer classroom content, and increased student retention and job placement rates. Students also explore information dynamically; are socially aware and more confident; communicate effectively about complex processes; become independent learners and self-starters; know their areas of expertise and share that expertise spontaneously.



Yet, even as school leaders understand these benefits and realize the need for a 1-to-1 program, many districts find their hands tied by budgetary issues and ongoing management challenges. BYOD programs, according to Impulse Point Chief Technology Officer Andrew Cohen, provide a logical, cost-friendly way to put technology into the hands of students. Learning increases with access and teachers are increasingly interested in leveraging technology; many are modifying their instructional plans to incorporate more digital experiences. Nearly a majority of classroom teachers (45 percent) noted in a recent study that they were creating more interactive lessons because of access to technology, an increase of 25 percent in just the past two years.

The Progression to Secure BYOD

It's recognized that a secure BYOD environment can enhance learning and instruction. A successful deployment, though, requires having the right security strategy, policy, and solutions in place that will ensure the integrity of district networks and resources.

Security has always been a top priority for school district IT managers. It's the reason most schools have operated within the confines of a managed device environment with network access limited to district-owned computers for administration and student labs—no personal devices were allowed on the wired network (as shown in the graph at the left).

As the requirement emerged to support the personal mobile devices of students and faculty, the use of an open SSID (service set identifier) was often deployed to satisfy early adopters. In this scenario, non-authenticated users gained restricted access to the Internet through a non-secure wireless network. However, this option lacked the identity management and security controls necessary to support the large number of users accessing the system once a district endorsed a BYOD policy. The introduction of learning management applications elevated BYOD to a core business function which requires a secure, scalable and predictable environment.

Secure BYOD enables faculty, staff and students to use their personal devices to access authorized learning management applications and Internet resources. It requires the end user to authenticate to allow for identity-based policy assignment and ensures compliance with the district's access and security policies. Adherence to these policies and the subsequent reduction in security risk and liability ensures a consistent level of service across both district-owned and BYOD managed environments.

Making the BYOD Policy Decision

How do school IT managers take advantage of a BYOD policy without adding complexity and straining support resources? How do districts allow personal devices and yet ensure that they are used for academic purposes? And how can IT managers allow personal devices access to network resources and protect them at the same time?

"Educators today want to take advantage of all that mobile technology has to offer in terms of engaging eager digital-age learners and promoting 21st century skills, but costs are often prohibitive," says Cohen. "Many districts are finding that BYOD policies can meet or augment their instructional goals in these tough economic times."

"A district of 10,000 students can suddenly find that 20,000+ devices are accessing the network, since most users own more than one device," explains Cohen. "But in the long run, districts are finding that secure network access maintains a successful BYOD environment for students, teachers and IT staff alike."

At **Napa Valley Unified School District** (NVUSD) in northern California, Laurel Krsek knew that higher education administrators grappled with these same questions when colleges and universities had to address the influx of student-owned devices and the demand for anywhere-anytime Internet access. So when administrators in her district began considering the idea of allowing students to bring their own mobile devices to school, Krsek turned to existing models in higher education for guidance. "We looked to see what types of solutions colleges had been doing because we didn't have the luxury of using an unproven vendor or solution," said Krsek.

Krsek and her team firmly believed that 1-to-1 computing was a necessity for 21st-century skills but felt that it was economically unfeasible. "It was obvious that we had to leverage students' personal devices," she says. "But we had to get everyone on board, gain consensus, and communicate to the school board, principals, and administrators that new policies would be crucial to protecting the BYOD environment. We held a series of focus groups with staff and teachers, and Impulse Point helped us through every step of the process."

One concern at NVUSD was the issue of equity for students who did not have a smartphone, tablet or laptop. The BYOD cost savings associated with not constructing computer labs allowed the district to provide hardware and software to many students and teachers who could not afford their own. NVUSD also decided on a peer tech support policy, since district staff were not permitted to work on student-owned devices.

In Harrisburg, Pennsylvania, the **Central Dauphin School District** (CDSD) also recognized the need for new acceptable use policies, and Matthew Sinopoli, director of technology services, developed a policy for the district's BYOD pilot program in fall 2012. The new policy "defines which, where, and how personal devices can be used to access the district network and outlines penalties for infringement," says Sinopoli. Enforcing such a policy required a solution that would be flexible and allows administrators to establish and edit network rules quickly and easily.

Selecting the Right BYOD Solution

When **Berkeley County K-12 School District** in South Carolina was considering a move to BYOD, the IT staff was naturally concerned about the security issues associated with 30,000 students and staff accessing the network from 37 remote schools. "Our biggest concern was keeping anti-virus, anti-spyware, and patches up to date. Additionally, we were concerned about the possibility of unauthorized devices being attached to our network without a reliable and consistent means of detecting and securing those devices," says Diane Driggers, director of technology for Berkeley County.

Requirements for a Secure BYOD Environment

1. Allow only authorized users to gain access to network resources
2. Identify which users are assigned to what devices on the network at any time
3. Ensure user devices are connected to a secure "encrypted" wireless network
4. Provide guest users with *limited* and *temporary* access to Internet only resources
5. Require that all personal devices meet a minimum set of security acceptable use policy standards and practices at all times to retain access privileges
6. Enable security and network managers to view all devices and user identities on the network in real-time. Historical information should be available for forensics and compliance reporting
7. Limit applications—including Skype and peer-to-peer file sharing software—and devices that detract from the learning and public safety mission of the district

In addition to addressing the requirements above, an ideal BYOD solution would also be cost effective, scalable, and require no incremental IT personnel to deploy and maintain.

The district needed a solution that could easily scale to support its remote sites without extensive hardware and integration requirements at each location or prohibitive costs. The solution also needed to support interoperability with the district's Cisco network infrastructure and Novell e-Directory Single Sign-On process. After reviewing several products, the district selected Safe•Connect and was quickly able to achieve a secure networking environment.

"Once Safe•Connect was deployed, we were immediately able to see where problems existed and get them corrected," says Driggers. Berkeley County was able to take advantage of Safe•Connect's scalability to support all its remote sites with a centrally deployed solution, ensuring easy management and scalability. "Other alternatives we considered required us to deploy one or two servers at each remote school location," commented Driggers. The district can now prevent unauthorized devices from accessing the network, stop the spread of malware, control peer-to-peer file sharing, and broadcast emergency messages to all or selected locations. "It's been a seamless experience for our users," says Network Administrator Jeff Winningham.

At NVUSD in California, Krsek realized within the first six months of BYOD implementation that the district needed network access control, because students with mobile devices were utilizing significant bandwidth for non-educational purposes. "When we first implemented the wireless network, we opened it up and wanted to see just how far it would go," she says. "But it soon became quite clear that students were bringing in personal devices to use on the network for purposes other than education. We were running out of bandwidth quickly." With only six technicians supporting more than 30 schools and nearly 18,000 students, the district had to find a solution that could be implemented and updated quickly and easily. "It was imperative that the solution we chose be extremely user friendly, cost-effective, and have an intuitive policy configuration manager. When I did my research, I liked the Safe•Connect architecture, and I found their pricing to be very reasonable," says Krsek.

Krsek and her team worked with Impulse Point to implement Safe•Connect across the district network in less than two weeks. "Their implementation team is great," she says. The Safe•Connect system now automatically enforces anti-virus software updates and security patches, on-boards new devices, and the managed support group handles all troubleshooting with little or no involvement by the busy tech team. "Safe•Connect helps strike a balance between preserving resources and maintaining a reliable high-speed network that enhances the learning environment for everyone," says Krsek.

Safe•Connect's unique managed-service approach allows schools to easily identify, authenticate, on-board, and control non-district owned devices in real time, as well as automatically address the constant influx of new devices coming on to the market. Even when students return to school after winter or summer breaks with new tablets and smartphones, Safe•Connect's managed service offering ensures a quick, efficient and cost-effective solution to fingerprint these new devices within 48 hours where other solutions may require a week or months of delay.

It is the managed support service included with Safe•Connect which enables school districts to implement a BYOD initiative even though they have limited staff resources. The Safe•Connect system becomes the eyes and ears for knowing who and what is on the network and is able to take automated action based on the district's computing policies. And the managed support service monitors the operation of the Safe•Connect solution, ensuring it is running properly and is automatically updated.

In Harrisburg, CDSD wanted to provide 21st century learning opportunities for its digital-savvy students, but needed an affordable alternative to funding a 1-to-1 computing initiative. Embracing a BYOD policy looked like a very viable option and the district's technology director, Sinopoli, knew that a mobile device management solution would be required. He reviewed several options before selecting Safe•Connect. "Safe•Connect became the clear choice based on its ease of implementation and management and on our budget. Because Safe•Connect is so flexible, we can support the authorization of new mobile devices by leveraging our existing router," Sinopoli says. "Also, Impulse made BYOD economically feasible for us over time, because they replace their hardware at end-of-life and base their software pricing on average device usage, not on the total number of users. They also include ongoing 24/7 monitoring and support." Like many districts, CDSD found that Safe•Connect, deployed and supported as a managed service, resulted in lower risk and a lower total cost of ownership.

Sinopoli was also looking for centralized management to ensure that students were using the network resources for educational purposes only. "While we don't control the student's device, we wanted to make sure they aren't using district resources to access social media sites, communicate during tests, or access the district's internal networks. With Safe•Connect, I'm able to maintain centralized control and easily set up rules that limit gaming, peer-to-peer, and streaming media activities on the student's computing device," he says. Sinopoli and his team discussed configuration issues with the Safe•Connect support staff in weekly conference calls and reviewed any project implementation steps for the upcoming week as part of Impulse Point's service delivery process. "The implementation was very smooth," he says.

Transitioning to BYOD: Doing It Right

While allowing students, faculty and staff to access the district network with their personal devices was once considered a high-risk initiative with little return, today's district leaders are finding new opportunities with BYOD. According to Project

Secure BYOD Best Practices

- Identify all computing devices (laptops, tablets, mobile phones) on the network
- Authenticate all users
- Ensure all devices are connected to a secure WPA2 Enterprise wireless network
- Provide the ability to self-provision, identify and track guest users
- Establish and enforce security policy standards
- Access real-time and historical reporting regarding device, user identity, and compliance with established computing security
- Maintain the system with automatic updates so that it can remain current on identifying devices and assessing endpoint security practices

Tomorrow, over a third of principals (36 percent) say that a new BYOD to school policy for students is likely this school year.

Here's what leading schools are doing to successfully transition to a secure BYOD-enhanced learning environment:

Step 1: Embrace and Promote BYOD. The "consumerization of IT" is here to stay. Focus on the benefits for both students and teachers that allow them to use their personal devices.

Step 2: Implement Acceptable Use Policies. Developing an ad hoc policy can be problematic to both morale and the service quality of the network. Let everyone know in advance what devices and applications will and will not be accepted. Implement—and enforce!—these policies for everyone, including students, faculty, staff, parents, and guests.

Step 3: Build a Secure, Scalable BYOD Infrastructure. Ensure that your network can handle the influx of devices to support your BYOD policy *prior* to implementation. Deploy a solution that will fully support your current infrastructure and scale to accommodate future expansion and additional mobile devices.

Step 4: Focus on the User Experience. It's ultimately not about the network or devices—it's about the users behind them. Following the steps above will help ensure that the process of using personal devices will be as problem-free as possible. The better the user experience, the better the learning experience.

References:

Page 1: Pew Research Center Survey.
www.pewinternet.org/reports/2013/teens-and-tech.aspx, dated March 13, 2013

Page 1: 2011 "Speak Up" report, Project Tomorrow, Irvine, California.
www.tomorrow.org/speakup/index.html

Page 1: National School Board Association, "Technology's Impact on Learning"
www.nsba.org/sbot/toolkit/tiol.html#Enhanced

Page 6: 2012 "Speak Up report, Project Tomorrow, Irvine, California.
www.tomorrow.org/speakup/SU12_DigitalConversion_EducatorsReport.html, dated April 19, 2013

About Impulse Point

Safe•Connect is known for creating a user experience is that is simple and intuitive. The system automates the acceptable use policies (AUP) of the organization in a "set it and forget it mode", which includes telling a user why their system is out of policy and providing them guidance on how to regain network access privileges on their own. This capability is essential to negating end user support calls to the district helpdesk.

The easy to use experience extends to how district-owned and managed devices connect to the network. Safe•Connect supports single sign-on (SSO) authentication for active directory domain systems, so that district faculty and staff members will simply continue to use their standard AD login authentication method and their user experience will remain the same. Safe•Connect can also provide real-time security assessment of managed devices in audit-only mode, which means that managed users will not be messaged or blocked due to noncompliance, but the security and network teams can monitor the security health of their device in a passive manner.

Deployed and supported as a managed service, Safe•Connect's rapid installation, network independence, and track record of reducing help desk calls results in lower total cost of ownership and reduced risk. Customers currently entrust the security of more than three million endpoints to Impulse Point.

To learn more, visit www.impulse.com

About T.H.E. Journal

THE Journal is dedicated to informing and educating K-12 senior-level district and school administrators, technologists, and tech-savvy educators within districts, schools, and classrooms to improve and advance the learning process through the use of technology. Launched in 1972, *THE Journal* was the first magazine to cover education technology.

THE Journal's franchise consists of the monthly print magazine (which is also available in digital format), the web site thejournal.com, six newsletters (THE News Update, T.H.E. Journal Insider, IT Trends, THE SmartClassroom, and School Security), and targeted list rental opportunities.

With a distribution of 100,000 circulation, *T.H.E. Journal* is the leading resource for administrative, technical, and academic technology leaders in K-12 education.

To learn more, visit www.thejournal.com

impulse

6810 New Tampa Hwy
Suite 400
Lakeland, FL 33815

(863) 802-3738

the JOURNAL

9201 Oakdale Ave.
Suite 101
Chatsworth, CA 91311

(818) 814-5277