DA District Administration
SOLUTIONS FOR SCHOOL DISTRICT MANAGEMENT

Creating a Robust and Safe BYOD Program

Plan to upgrade your district's infrastructure for increased capacity and security.

By: Ron Schachter
District Administration, April 2012

Until recently, student electronic devices, from cell phones to iPods to laptop computers, were the forbidden fruit in schools. But with technology budgets languishing and such devices becoming more powerful, affordable and omnipresent in students' lives, district technology leaders are now eyeing a welcome educational harvest through bring-your-own-device (BYOD) programs.

Lucy Gray, project director of the Leadership for Mobile Learning Initiative at the Consortium for School Networking (CoSN), has studied early BYOD adopters. "I'm stunned by the number of school districts opening their minds to this approach," she says.

High school, middle school and even elementary school students in a growing number of districts are being encouraged to bring in the very electronic equipment they were once admonished to leave at home. "There was a certain inevitability, as these devices became more common and cheaper, that at some point kids would be bringing them to school," explains Tim Wilson, chief technology officer for the ISD 279-Osseo Area Schools in Minnesota. "If something's coming, we might as well invite it in and learn to manage it."

To hear Wilson and other tech directors tell it, these devices are more than welcome. Wilson's BYOD program is called Copernicus, after the astronomer who proved that the sun was at the center of the solar system. "This is our attempt to put students at the center of our technology integration," he says.

In Minnesota, Wilson is overseeing the third year of a BYOD program, which took root at three high schools and five classrooms in the district's elementary schools. "We started small and let it grow organically," he says. The number of student- and teacher-owned devices has grown to over 3,000. While that number is a fraction of the Osseo Area's 21,000 students spread across 25 schools, the influx of student-owned devices is already making a difference.

"Some classrooms might have half the kids with devices and others just a handful," Wilson notes, adding that every year after Christmas break, a new supply of student-owned devices comes into the schools. "The students will share devices, and in lots of situations, that encourages collaboration among them. Our school district cannot afford a one-to-one computer program. The BYOD program allows us to use our own resources and to supplement them [with student devices]."

In the 180,000-student Fairfax County (Va.) Public Schools, meanwhile, almost 60,000 student devices have become an integral part of the school day – one of the largest such deployments in the country. The district's chief information officer, Maribeth Luftglass, hopes that, over the next several years, nearly all the students will bring their own devices. "Our hope is that if kids bring enough devices, it will help us with our underfunded cycle for refreshing computers in the classroom," she says.

Along with a one-to-one middle- and high-school laptop program for the Tri-Creek School Corporation, a five-school district in Indiana, Jay Blackman, the district's director of information and technology, also has made a place for student devices. "We encourage BYOD as a supplementary program," he says. "We're starting to see a growing number of students bringing laptops, iPads and iPods into the classroom."

Building Network Capacity

Those who have launched substantial BYOD initiatives, and those who study them, are quick to point out that while these programs may become educational game-changers, they are also changing the rules when it comes to network capacity and security. "We know that districts are going to have to upgrade their infrastructures to accommodate much more traffic," observes Karen Cator, director of the Office of Educational Technology at the U.S. Department of Education. Two years ago, the Federal Communications Committee released its National Broadband Plan, which is aimed in part at doing just that, and making E-Rate funds more flexible to include such devices as smartphones.

The Osseo Area schools provide comprehensive Wi-Fi coverage so that all students can reach the network, but Wilson cautions, "Coverage is not the same as capacity. That's an important distinction as these programs grow." Wilson explains that if too many of the BYOD program's 3,000 devices tap into a single access point or a number of those devices are downloading videos, then the entire Wi-Fi network can be affected. "My network team's work is identifying the parts of the school where lots of these devices are showing up and hearing from students and teachers about how well they perform." When there is an overload, the IT staff can redistribute the bandwidth. If necessary, Wilson can purchase additional access points at $1,500 each and, eventually, may spend thousands more on an additional controller as those access points proliferate.

In Indiana, Blackman's IT team monitors the Tri-Creek School Corporation's network for how much bandwidth individual devices use. "We're able to set up levels of access," he says. "For instance, YouTube use may be limited at certain times of the day to make sure our bandwidth is not eaten up by YouTube users."

Network Security and More

Don Knezek, executive director of the International Society for Technology in Education (ISTE), notes that starting a BYOD program means making adjustments when it comes to security, especially protecting a district's proprietary and secure data. That function, he says, used to be handled by an effective firewall that kept out unwanted users and their devices.

"Nowadays, you have to have a layer past the firewall that we didn't have to deal with when we simply said no to user-owned devices," he says. "Now all of a sudden, you have multiple points of entry at different levels of access, and that requires more diligence."

One key to maintaining adequate security, Knezek and other experts say, is to have multiple networks: one for Wi-Fi traffic, one for district business and for other secure information for teachers and administrators only, and one for students and outside users of the district's Web site.

"Students are not getting access to our internal network and resources," Wilson explains. The devices in the BYOD program do not have the district's printer software installed, since printers reside within the district's internal network. "If we did get them on the printers, that would require providing access to our internal network," Wilson adds.

Jared Lynn, technology coordinator for the PORTA Community Unit School District #202 in Illinois, is taking the same approach while planning for a BYOD program in the next year or two. "Our entire wireless network goes out its own port," he says. "There's no connection to printers or any school content."

In this way, BYOD content and other content travel as if on separate railroad tracks. The wireless devices of teachers may share the same track as the student devices. In that case, it becomes necessary to "write policies" for the network hardware – programs that allow teachers to cross over into the track leading to restricted areas. The challenge for IT departments is making those instructions foolproof.

"On most security systems, [this capacity is] available but not activated. [Network administrators] haven't accessed that level of sophistication," says Knezek. "They need to create a different set of policies that say, 'This is OK, but this isn't.' And if your current version of equipment doesn't have all the security features, the next upgrade will."

Districts such as Tri-Creek, Fairfax County and the Osseo-Area Schools are increasingly using "platform neutral" Web 2.0 applications such as Google Docs, Edmodo and netTrekker for teacher assignments and student work and collaboration. These applications not only work for any device that has a Web browser, but they also help with security by processing and storing any work at those sites in the cloud, away from a district's servers.

Districts may also need to rewrite acceptable-use policies banning the use of electronic devices inside the classroom or on school grounds. However, the long-held concern about appropriate and safe Web content still needs to apply, say the experts. "It's a challenge to make sure that students are safe online, using school-issued devices or a BYOD," notes the DOE's Cator. "Make sure the appropriate rules are in place, and have students sign an agreement to abide by those rules." Wilson also points to a more mundane security concern, for which he coaches teachers participating in the Osseo Area BYOD program, of making sure that unattended devices do not go missing. "If you're walking kids down to music class [and they leave their devices in the classroom], you have to lock the door," he insists, adding that the district had considered installing locked cabinets for the devices in the classrooms but dismissed that solution as too cumbersome.

Limiting the Costs

These tech leaders also point out that running a BYOB program does not carry major costs, unless it is necessary to expand the bandwidth or Wi-Fi reach of the existing network. They would have purchased the same equipment to meet their networking needs, they say, even without a BYOD program. Of course, schools and districts without a Wi-Fi network in place would have to pay for the necessary access points and controllers to set one up.

Last year, Blackman installed a new generation of Hewlett-Packard switches and hubs to increase Wi-Fi capacity, while Fairfax County's Luftglass uses a combination of Aruba and Cisco products. The equipment driving the Wi-Fi network for the Osseo Area schools comes from Extreme Networks.

When it comes to student equipment, Wilson says, "tech support is easy because we don't provide it. If there's a problem with one of the devices, the student takes it home and the family helps fix it." More often, he says, students or their classmates are already experienced in handling technical problems. The IT department also sends home a standard disclaimer letter noting that the school is not responsible for any broken or stolen student devices. The district is not alone, as many district IT teams can't keep up with the diverse and multitudinous devices.

While Blackman's IT department does provide support for the BYOD devices in Tri-Creek, he admits, "We don't get a lot of calls, because students are turning out to be the best tech support." Besides raising technical concerns, running a successful BYOD program can come down to revising or enforcing an acceptable-use policy. "Be aware of what exists at your district policy level," Wilson suggests, adding that teachers also need to make clear to their students when devices should be on during a classroom activity or off and out of sight.

In Fairfax County, students participating in the BYOD program complete a formal registration, Luftglass says. "We wanted to make sure that students and parents agree to the rules and regulations," she explains, noting that the registrations database helps identify problems. "If someone is downloading huge amounts of video and clogging the network, we can quickly find the device electronically and match it to the database."

At that point, the IT department can ask the user to cut back.

Early Reviews

The early reviews for these emerging BYOD programs have been positive. "If you talk to the teachers participating, the vast majority of them say the BYOD program is great," reports Wilson. "We'd love to see more kids bringing in devices."

In Fairfax County Public Schools, Luftglass has bigger plans, as well. "We think that, eventually, 90 percent of our students will bring in devices as they get cheaper," she says. "We think this program will grow and grow."