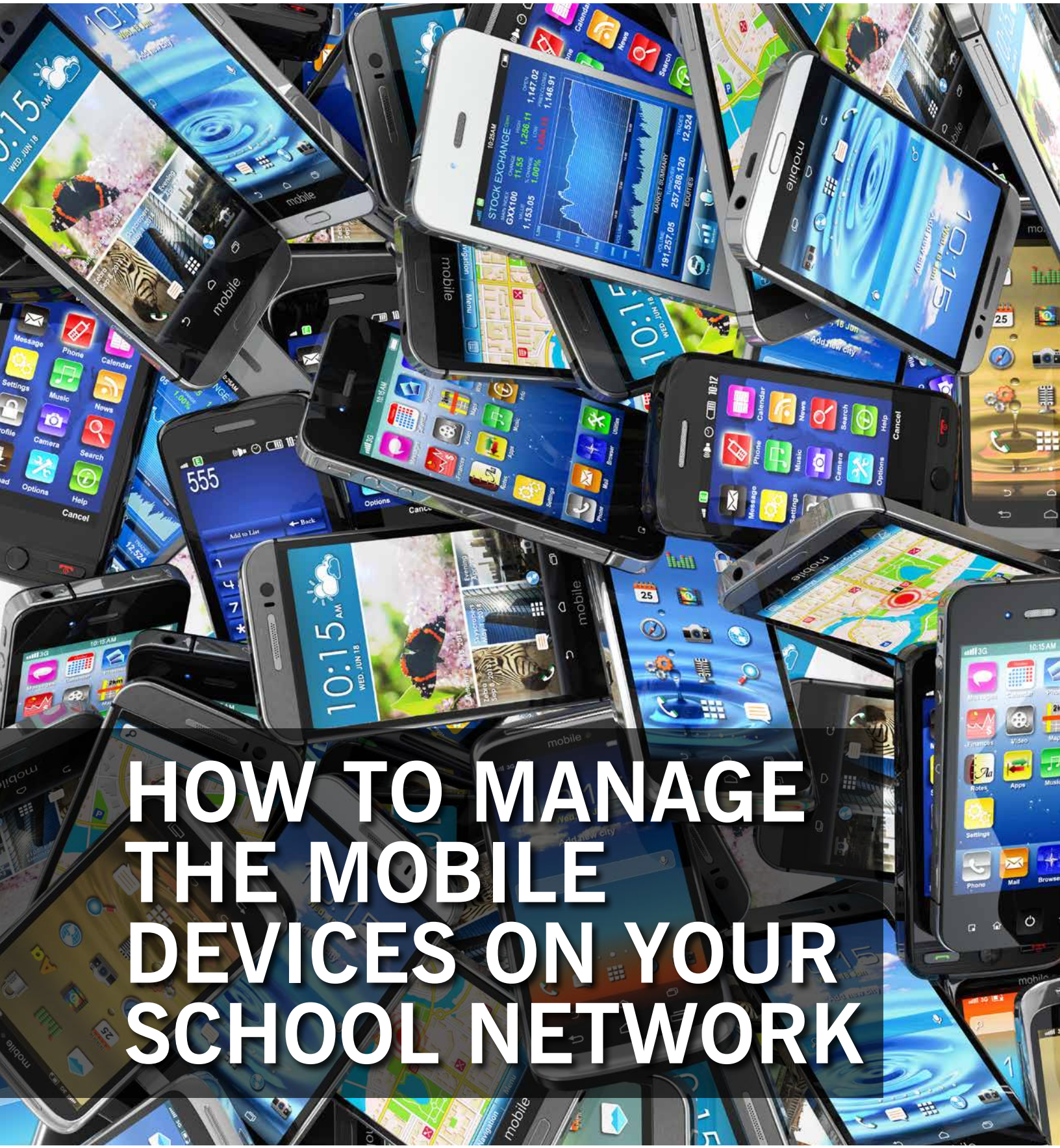
DEEPDIVE

K-12TechDecisions



HOW TO MANAGE THE MOBILE DEVICES ON YOUR SCHOOL NETWORK

How to Manage the Mobile Devices On Your School Network

Beefing up Wi-Fi is only the first step in MDM. We walk you through provisioning devices, deploying applications and more. ***BY CRYSTAL BEDELL***

BY NOW, K-12 SCHOOLS KNOW the value of getting devices into students hands. It doesn't matter if it's a laptop or tablet, access to technology opens the door to so many things like creation, collaboration and personalized learning. The challenge lies in figuring out how to manage the additional devices once they hit your network.

This resource is designed to help you with that. We'll walk you through everything you need to know before any device even logs onto your network. Learn more about the important decisions that lie ahead once you make the commitment to go BYOD or 1:1 in your classrooms.

WITH THE RISING POPULARITY of 1:1 and BYOD programs in K-12 environments, school IT managers are increasingly tasked with implementing and managing mobile devices on the school network. This presents a number of challenges, not the least of which is giving a diverse user base the freedom to learn and innovate even as it continually tests the IT department's control.

"The user base will challenge you everyday. They will find new ways in and around everything you put up," says Michael McNamee, senior network engineer for Secure Edge Networks, a Charlotte, North Carolina-based wireless service provider. "The kids will find new uses for the technology and find ways around the barriers you put up to do whatever they want to do on your network with your devices."

McNamee has seen students share inappropriate content using AirDrop on an iOS device. He's also seen students use screen sharing on a Mac to have one student take a test for another. Of course, kids will be kids and their intent isn't usually malicious, but if they can find a way to get out of class work, they probably will. This raises the issue of how to manage a classroom once devices have been introduced.

Thierry Karsenti, professor and research chair at the University of Montreal, has studied this issue with tablets in the classroom. "When teachers ask students to go on a website, it takes time. They start to do something else. They find a way to go on Facebook, find games, answer text messages and so on," Karsenti says.

As chief technology officer for Highline Public Schools, Mark Finstrom knows the challenges of mobile device management well. He supports 20,000 students across 34 schools. "Kids are always testing. They're always asking, 'What can I do to render this device useless so that I can use it in a different way?'," he says.

But, this doesn't stop Finstrom from allowing a variety of devices on the schools' network: Chrome OS, iOS, Mac OS and Windows. The district both provisions devices and supports BYOD for those students who wish to use their own.

Things to Consider Before You Deploy Devices

Before students are given devices or are allowed to bring their own devices to school, IT must ensure that the network has the capacity and controls to handle the additional traffic.

"Devices don't have Internet ports anymore. There's no wired component to fall back on, so you need a really robust and feature-rich wireless platform. Without the security features on your wireless, you're going to have some unconquerable challenges from your devices, especially with BYOD," McNamee says.

Schools should also have a content filtering solution at the edge of the network. McNamee recommends one that integrates with the school's wireless platform to create a seamless end-to-end security path.

If you've decided to provide your students with devices and will allow them to take those devices home, you need to decide whether you will secure the device both on and off the school network. There isn't a right answer here. It really depends on your student body, the culture at your school and how you view the role of technology.

The technology department must also consider how to provision devices and create some sort of authentication to the school network. "Provisioning also includes naming, registering and documenting devices," McNamee says. "Those things don't happen automatically."

Then there's apps to think about. Should individual teachers download the app they need onto the students' devices? Should students do it? Or, should that task be completed at an administrator level where applications can be pushed out and updated through mobile device management software?

It depends on the schools and their technical ability," McNamee says. "Some teachers want to have the control of the apps they are using for curriculum delivery so that's fine and dandy for them; however you have some teachers where that's not that in their wheelhouse, so they need some hand holding and training."

If the school district is provisioning devices, then much of this can be achieved using a mobile device management (MDM) solution. "It makes the roll-out process a lot easier. It also makes securing and controlling the devices much easier, whether they are on the internal network, at home or on other networks," McNamee says

An MDM solution also helps reduce the district's liability. "As long as you put an MDM solution or app on the device, use best practices from that MDM vendor, and do your due diligence, I don't think anybody would fault [the school] if a kid found a way around [the MDM solution] in a one-off instance. It would be negligent if the school didn't put MDM on the device and a student used it however they wanted," McNamee adds.

It's also important to make sure your MDM solution supports all platforms, whether iOS, Android or Windows. In Finstrom's case, this means using more than one tool. "I have to be nimble and flexible with the tools I use. Not one MDM solution is going to meet all my needs. I have multiple solutions. That seems unwieldy to some people, but to me that's the normal course of action," he says.

McNamee also suggests looking for a tool that provides the abil-

ity to set up different security profiles. “When the device is at school you may not need to secure it as tightly because you have built-in security on the wireless and wired networks and a firewall on the Internet. But when a student goes home, on the network, you don’t know what that environment is like so you need to lock it down even more.”

How to Manage BYOD

While MDM is a must-have for district-owned and -provisioned devices, it doesn’t solve the challenge of managing student-owned devices in a BYOD environment. “I don’t install anything on a student or parent device. That is purposeful. That is not my device. I may have management concerns, but I don’t have licensing availability. Many licenses don’t allow us to install on student owned devices,” Finstrom says

In addition to licensing issues, schools don’t want the responsibility. “As soon as an MDM app is on the device, it becomes [the district’s] problem, and they have to support it,” McNamee says. “They’ll be getting the call to fix it if something goes wrong.”

Because IT lacks visibility into student-owned devices, IT managers can’t fully know what they’re getting into once BYOD goes live. However, schools that successfully manage BYOD typically use a wireless solution and some sort of web content and malware filtering on the firewall to lock down the access BYOD devices have on the school’s network. While the idea of going BYOD may seem a bit like entering the wild west, it doesn’t have to be that way if you do your due diligence and really prepare.

“From a security standpoint, if you have the infrastructure in place to lock things down, BYOD is not a challenge or a threat,” McNamee says. “If you don’t have the infrastructure in place, BYOD can be a big headache.”