Kaseya White Paper

Mobile Device Management and Bring Your Own Device in Education Environments

Mobile devices have the potential to engage students in new ways, but IT often doesn't know how to manage the new technology in a way that cultivates an innovative and supportive learning environment while staying true to the organization's IT and security policies.

Kaseya

www.kaseya.com

There are now more than 4.6 billion mobile phones in the world[1], and children under 12 years of age constitute one of the fastest growing segments of mobile technology users in the U.S.[2] According to Project Tomorrow, two-thirds of high school students own a cell phone that has Internet access while one in five kindergarten through second graders do as well (see chart below).[3] Teachers are also using mobile technology—smartphones and tablets—as innovative teaching aids in the classroom, using them to create curriculum, grade assignments and track student progress.

Students are Embracing Mobile Devices

	K-2nd grade	3rd-5th grade	6-8th grade	9-12th grade
Cell Phone (without Internet access)	18%	29%	59%	67%
Smartphone (with Internet access)	14%	17%	24%	31%
Laptop/Tablet PC	27%	32%	53%	60%
Netbook or mini-notebook computer	n/a	n/a	11%	10%
MP3 player	36%	55%	80%	85%
Hand-held game player	47%	60%	64%	48%

There is an amazing opportunity to engage students with mobile technology on their terms, using the same devices that are used for texting their friends and playing video games to get them excited about history, math and science. However, there is a tendency among K-12 IT organizations that mobile device adoption won't jive with existing IT and security policies. The result is a knee-jerk reaction to push back on this nascent technology.

The challenge that IT must figure out is how to manage and secure mobile devices while cultivating an innovative and supportive learning environment.

This is going to require a sea change in how education IT professionals support users. IT used to be a technology gatekeeper, dictating what devices and computers could be used. With the advent of mobile devices and specifically a new Bring Your Own Device (BYOD) mentality, IT now needs to be more collaborative, working with teachers and students to identify and support the tools they need.

> "The reality is that the use of mobiles continues to be restricted by policies that prevent many schools from taking advantage of them as tools for teaching and learning."
>
> – Learning in the 21st Century: Taking it Mobile!

Three Common Issues with Mobile Device Management (MDM)

The problem with mobile device management is that it is new and represents a different way of providing IT support to users. Education IT professionals often lament three main challenges that they face with mobile device management.

1. Volume: Mobile device adoption almost always means bringing on hundreds or thousands of new devices under the management umbrella. Teachers are increasingly relying on mobile devices and, a one-student-to-one-device ratio is growing increasingly common. Not only that, but not all of these devices are running the same OS. How do you even know what devices are connected to the network? How are these devices being used and by whom? Can you scale effectively to meet growing demand?

2. Labor: Bringing hundreds of new devices under the management fold is complex and time-consuming. Mobile is a new technology that often requires additional policies and procedures to maintain availability and performance. Administrators need to be trained on new tools while users need to be educated on new policies and terms of use while knowing how to get their personal devices connected to the network. How do you do this effectively? How do you apply policies to mobile devices that you don't even own? How can you ensure thousands of devices are being managed effectively without adding staff?

[1] International Telecommunication Union February 2010 Press Release
[2] Pockets of Potential - Using Mobile Technologies to Promote Children's Learning, Carly Shuler, The Joan Ganz Cooney Center at Sesame Workshop, 2010
[3] Learning in the 21st Century: Taking it Mobile! Blackboard K-12 & Speak Up 2010 Report. Project Tomorrow

3. Security: Protecting devices from infection and preventing data breach is still paramount. Only the platform has changed. How do you enforce security policies on mobile devices that move in and out of your network? How much of a risk do they pose to the rest of the environment? Should mobile policies for teachers' devices be different than students' devices? What about lost or stolen devices? Are there procedures in place to recover or wipe those devices?

How to Choose the Right MDM Solution

If you already have a robust IT systems management strategy in place for your traditional infrastructure (such as desktops, laptops and servers) - why reinvent the wheel? Existing policies and procedures can be easily extended to mobile devices, but you have to have the right tool to make it work. If you haven't deployed an integrated IT systems management solution, you should consider it. The right tool can consolidate monitoring, maintenance, backup and security for all your systems—regardless of platform, OS or physical location. The solution should provide you with detailed and holistic management data on a single pane of glass, giving you and your administrators the visibility you need to enforce policies and conduct regular maintenance. Much of the manual administration associated with MDM should be automated, providing cost-effective IT systems management across the entire environment—even for devices not procured by the school or district.

Drew Lane, director of technology for Derby (Kansas) Public Schools, successfully developed a MDM strategy though which he has been able to take a proactive, preventative approach to mobile devices, making it easier for users and his staff to find and fold mobile devices in the district's management umbrella.

"Implementing the right MDM strategy has allowed us to create operational efficiencies, expand management functionality and empower teachers and students with powerful learning and teaching tools," he said.

Here are solutions to the three common MDM challenges outlined above:

Solving the Volume Issue with Auditing and Inventory

The right MDM solution should enable the management of thousands of mobile devices by providing both a holistic and drill-down view into all systems in your environment. Agent-based solutions give administrators complete visibility into each device, including serial number, operating system, firmware status, installed applications and other inventory data. The solution should also have probe capability that gives you a holistic view of the network as a whole. Management and inventory data should be updated automatically in real time and be available live via dashboard or in detailed management reports. This auditing and inventory functionality gives school districts a comprehensive, real-time overview of all mobile devices in your environment.

Solving the Labor Issue with Profile and Policy Management

Another key capability is to ensure policy enforcement by consolidating management functionality in a single, Web-based solution. Through integrated solutions, administrators can centrally monitor Wi-Fi connectivity, enable email configuration for common protocols such as Exchange, Gmail, POP and IMAP and automatically push out security settings. Administrators can even activate or deactivate factory default options and applications and assign profiles to one or many mobile devices through the air. A solution like this standardizes mobile device management and eliminates many of the manual, labor-intensive administration associated with regular maintenance. These operational efficiencies enable a flexible yet consistent mobile device policy and allow IT staff to focus on other, more strategic projects.

Solving the Security Issue with Geographic Location Tracking and Loss or Theft Handling

One of the most important features of your MDM solution is the ability to secure mobile devices. By consolidating security management of all devices on a single management dashboard, integrated solutions ensure there are no security holes in the network and policies are applied

MDM Advice for K-12 Environments

Drew Lane, director of technology for Derby (Kansas) Public Schools, has developed a successful mobile device management strategy for his district. Here are four tips he wishes someone would have told him before he started the project.

Have a Plan:
Don't be surprised when iPads start showing up in your environment. Be proactive by developing IT and security policies and procedures for all mobile devices.

Incorporate MDM in Overall Campus Workflow:
Users need to understand that if they are going to log into the school's network or use WiFi, they will need to agree to let IT manage, secure and protect their personal device.

Run a Pilot:
Test your environment. It's much easier to make changes when you're dealing with 12 devices rather than hundreds or thousands.

Be Patient:
Mobile technology is still new, and everyone is still figuring out how everything fits together. Mistakes will be made. This will take time. You'll eventually get there.

consistently and efficiently. The solution you choose should also enable geographic location tracking for mobile devices that include on demand location query and historical device location tracking on an intuitive, easy-to-read map-based interface. For lost or stolen devices, it should be able to remotely sound an alarm on the device, lock it down, wipe the memory and hard drive, reset to factory settings and even automatically create a ticket when the device checks in. Bottom line, it should provide the capability to recover mobile devices quickly or render them unusable if unable to be recouped.

Contact Kaseya Today

Mobile technology has the potential to revolutionize our education system for both teachers and students. IT needs to develop a plan to deal with an increasing amount of mobile devices logging on and off education networks—many of which have not been procured by the school or district.

Visit **http://www.kaseya.com/industries/education-it-res.aspx** to learn how Kaseya provides administrators the visibility into and control over all devices in education environments.

Visit **http://www.kaseya.com/features/mobile-device-management.aspx** to learn more about the Kaseya Mobile Device Management module.

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to www.kaseya.com/download for a FREE trial.

Visit: www.kaseya.com | Email: sales@kaseya.com | Like: Facebook.com/KaseyaFan | Follow: @KaseyaCorp

Drew Lane's Five Features to Look for in a MDM Solution

Activation:
Associate new device with your environment.

Enrollment:
Associate new device to account and bring it under management.

Configuration:
Apply settings via configuration profiles.

Security Management:
Set up ability to lock, remove passcode or wipe device.

Inventory:
Set up the ability to know where devices are and what they contain.

> “The right MDM solution should enable the management of thousands of mobile devices by providing both a holistic and drill-down view into all systems in your environment.”

Kaseya

www.kaseya.com