Managing Mobile Devices in **K-12 Environments**

Faronics™

Executive **Summary**

Technological innovations like mobile devices have revolutionized every sector within the modern world. With trends like the bring-your-own-device phenomenon massively improving productivity and effectiveness in many private companies, it's no surprise that educators want to utilize mobile devices.

In fact, a study published in The Journal found that around 49 percent of teachers surveyed in 2015 had school-issued mobile devices in their classroom.

While the advantages of this move are clear, introducing gadgets like smartphones and tablets into schools brings a number of headaches for the IT department. The obvious solution for many has been to implement a device management system, but these programs aren't all created equal.

What's more, many focus on the problems inherent with Apple devices as they are often the most popular - while skipping over concerns associated with Android or Chrome OS devices.

To that end, let's explore general problems schools run into with their device management solutions along with other issues they encounter during mobile device deployment.

MDM **Challenges**

To begin, it’s important to recognize what school administrators are up against when allowing mobile devices in the classroom.

Perhaps the best example of this is what happened in the Los Angeles Unified School District (LAUSD) in 2013. According to the LAUSD Chief Information Officer (CIO), concerns emerged surrounding the school-issued iPads that students were allowed to bring home.

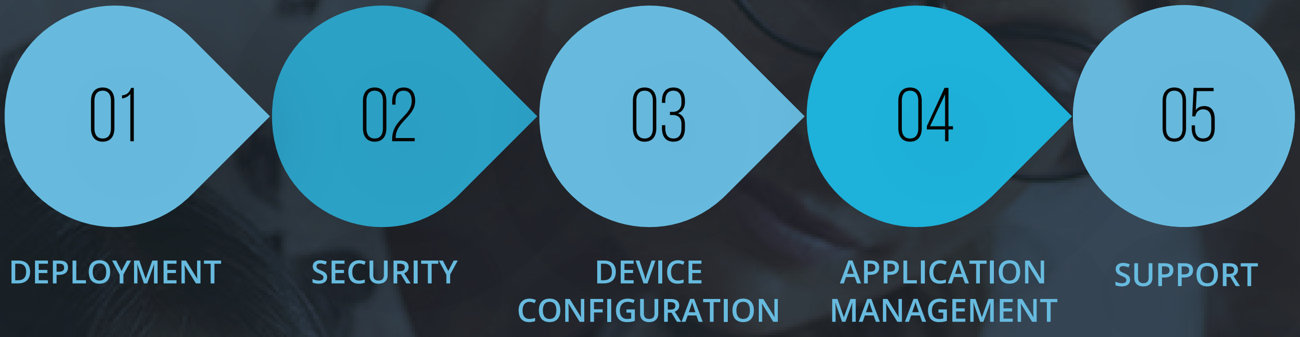
Although the district had implemented mobile device management software to prevent students from accessing unapproved websites and from downloading unauthorized mobile apps, the students found a way to circumvent that system.

In fact, all they had to do was to delete Apple's Global Proxy that routed all their traffic to a comprehensive filter.

While the fallout was certainly insignificant – 340 students were able to access the internet unfiltered for one night – this story highlights the importance of robust security tools for schools. Students can be impulsive and implications of certain actions can result into unwanted liability for schools, and it's therefore up to the schools to set finite boundaries.

This brings us to an important point. How can school IT teams enable productive learning in classrooms, with minimal distractions, while embracing mobility in education, and most importantly, addressing the ensuing challenges and understanding the aspects of mobile device management (MDM).

MDM in Schools : **5 Core Aspects**


01 DEPLOYMENT

02 SECURITY

03 DEVICE CONFIGURATION

04 APPLICATION MANAGEMENT

05 SUPPORT

Deploying the MDM solution

When handing out these devices, students need to be made aware of the massive risks involved. This could be as simple as a lecture from a teacher or could go as in-depth as a homework assignment about security, but the fact of the matter is that students must be made aware of the stakes.

Platform security

It's up to administrators to focus on platform security. According to Techopedia, platform security surrounds the need for architecture and processes created to ensure the safety of the entire computing platform. It will be up to IT officials to help construct the exact nature of this ecosystem, but the point is that platform security is of the utmost importance here.

Setting up the device configuration

Another important point to discuss is how app deployment is going to affect device configuration. Each school and classroom is going to have different needs, but the key is to ensure that everything is able to work together.

Managing mobile applications on the devices

You'll have to invest in robust mobile app management. These platforms allow you to have more control over what's going on with school-owned devices as well as how that might affect overall configurations.

Support during implementation

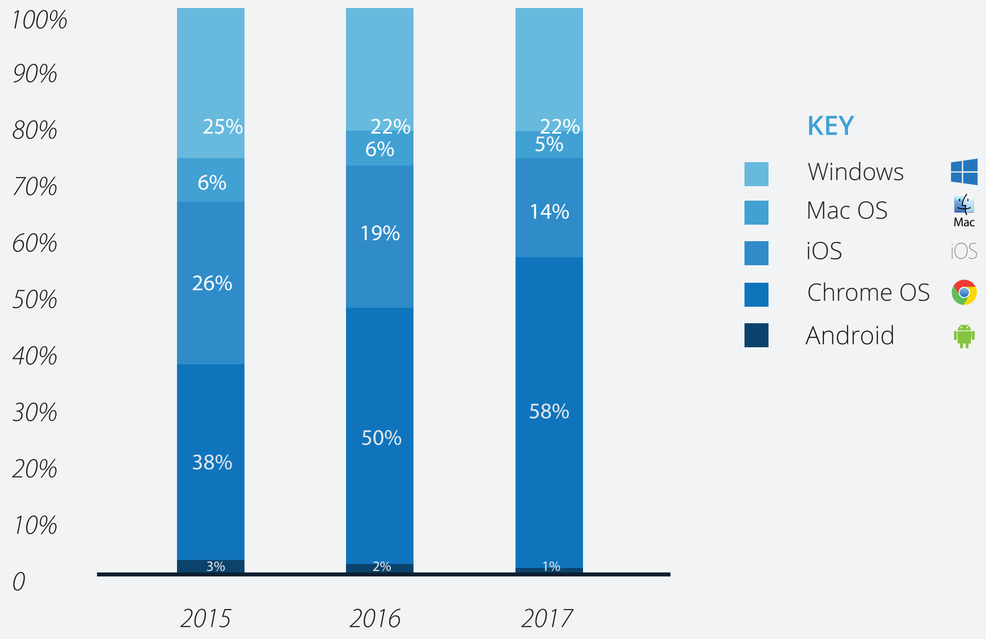
You'll need a lot of help from a knowledgeable source. This support is crucial for a proper deployment of any system, including mobile device management solutions.

K-12 Education Environments

With so many devices to choose from, it makes sense for IT administrators to first survey which gadgets others in the field are using.

The Mobile Device Landscape

According to a report by Futuresource Consulting, **Chrome OS had 58%** market share of K-12 schools in the United States. On the other hand, Apple's **iOS had 14%**, while laptops with **macOS had 5%**. **Android had** a **1%** share, maintained.

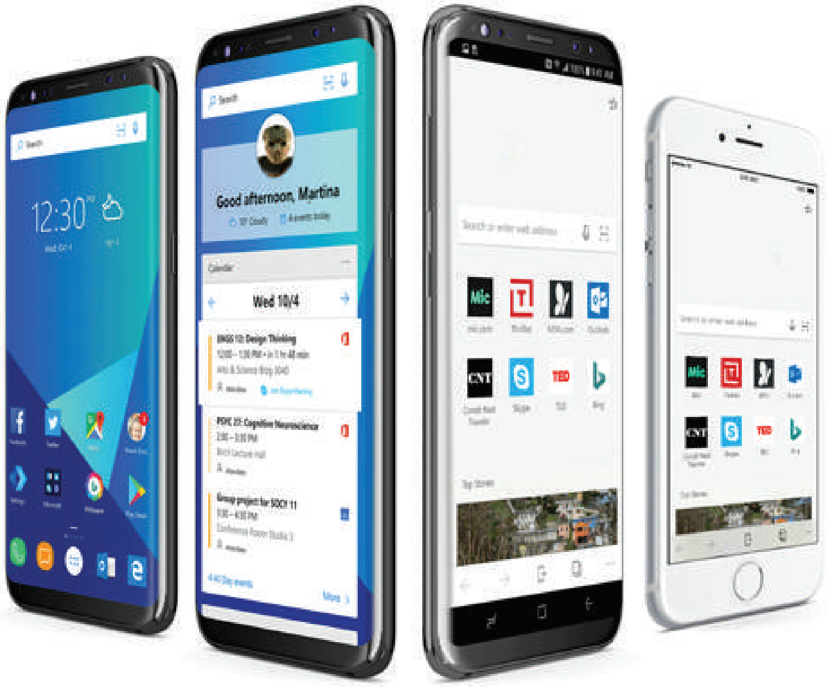


K-12 Mobile Computing Units - Annual Shipments - **United States**

Although iOS, Chrome OS and Android powered devices are working hard to keep users safe, many within the field still believe Apple to be the safer choice of the three most popular platforms.

ZDNet's Conner Forrest reinforcement this statement when comparing the 3 platforms, pointing to Apple's control over "the entire device ecosystem" as a reason for the company's perceived security dominance. By maintaining a tight grip on firmware, software and hardware production, Apple has more control over security features.

Forrest also pointed out that Apple's fight with the FBI over its iOS encryption bodes well for consumers. In fact, this incident only prodded Apple to increase security. However, this doesn't mean that Android devices are inherently unsafe. In fact, Forrest went on to say that Google's commitment to delete harmful apps from its app store and its automatic security updates are major advantages to using Android. Chrome OS takes security a step further, since Chrome apps run live from the cloud, the OS doesn't run executables. Therefore, theoretically no traditional virus can be installed on a system.



iOS vs **Android** vs **Chrome OS**

With iPads being one of the the most widely deployed mobile devices in K-12 environments, school IT admins come across the following mobile device management terms frequently.

1

DEP - Device Enrollment Program

Apple's Device Enrollment Program (DEP) automates enrollment into MDM during the Setup Assistant process for devices purchased through Apple.

2

VPP - Volume Purchase Program

Apple's Volume Purchase Program (VPP) allows schools to buy apps in bulk from the Apple App Store.

3

OTA Enrollment

Over-the-Air Profile Delivery and Configuration delivers a profile to a device. This enrollment option allows a server to validate user's login, query for information about the device, and validate the device's built-in certificate.

4

Managed Apple IDs

Educational institutions can create Managed Apple IDs for instructors and students to use for educational purposes. IT admins can manage the services that your Managed Apple ID can access.

5

Shared iPads

Students are assigned to specific shared iPads via Apple Classroom using unique Apple IDs. School IT admins get the ability to create a 1:1 personalized device experience even though the device is shared.

Security : **Mobile App Management is Necessary**

Any school wishing to utilize Android devices should understand what they're getting into. According to TechTarget, one of the biggest challenges to Android device management is the plethora of malware targeting these gadgets.

While these cyber attacks can come in many forms, an important vector for schools to focus on is app management. This is the exact kind of cyber attack that young students could fall for. It's so easy to simply download an interesting app without thinking about the consequences.

The fact that the school would be charged rather than the student could allow such a crime to go unreported for some time.

TThe solution is to utilize a device management platform that enables the administrator to quickly and effectively remove unwanted apps or changes from a device, while ensuring only vetted/ approved apps go through.

Administrators need to have complete control over the app and software allowed on school-owned devices. Unfortunately, end-users and especially students cannot be entirely trusted to make the right decision when it comes to downloading something from the internet.

Mobile App Management (MAM) can be tricky for school IT teams, but with the right tools, a lot of time and effort can be saved.

BYOD for **Schools**

According to the Pew Research Center, **73 %** of teens in North America **owned a smartphone.**

Although mobile device deployment within K-12 education is generally thought of as an attempt to get school-owned devices into the hands of students, many have started to see the benefits of telling children to simply use their own phones, tablets and computers. This trend, also known as bring your own device or BYOD, has gained a lot of traction in the enterprise, but it also has applications within education.

On the surface, BYOD can seem like a bad idea. Some might say that encouraging students to use their own gadgets in school will result in a rush of short attention spans. However, this completely ignores the fact that students are already using their phones in the classroom. In fact, taking the secrecy out of it might even help with students see their phone as an educational tool rather than a communication device.

Additionally, a BYOD program might actually help decrease the number of issues IT has to deal with. People generally take good care of their own devices as opposed to ones they've been given, and the personal ownership aspect of BYOD might help IT administrators avoid fixing mistakes made by careless students.

Finally, but perhaps most importantly, BYOD is simply more cost-effective than purchasing devices for each student. According to Pew Research Center, 73 percent of American teens had access to a smartphone in 2015. This means that a vast majority of a school's student body already have the gadgets districts want to buy for them, so simply requiring them to bring them in from home just makes sense.

The Need for Unified Endpoint Management **in K-12 Environments**

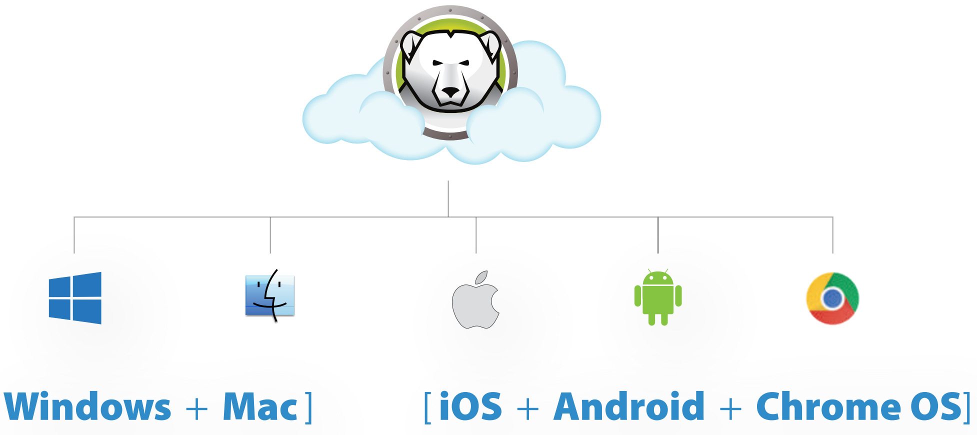
With all the chaos the educational system creates, it's important for IT administrators to hold a certain level of control. This is especially true for the technology used within the school, and it's why centralized management of endpoints - PCs and mobile - is important.

Modern IT has become too complex to be managed efficiently through multiple interfaces. To simplify and streamline the process, an integrated management suite is recommended as it allows school IT teams to control devices from a centralized console. By securing all endpoints within the organization, IT teams get a more granular hold on their environment.

UEM can simplify many endpoint maintenance and management challenges for IT teams of large or unified school districts.

Even within in a single school district, each school is different and might choose varied devices depending on their specific learning needs.

With school IT teams having to deal with Macs, Windows PCs, Chromebooks, iPhones, iPads, Android mobile devices, keeping it all together is difficult without a centralized control point. Faronics Deep Freeze Cloud offers an intuitive console which can manage all your different devices for your entire institution with ease.



Faronics' end-user driven approach to endpoint management allows administrators to keep track of a multitude of devices across large or small school districts. Faronics Deep Freeze Cloud platform's UEM capabilities allow for management of lab room PCs, student mobile devices, staff workstations, BYOD gadgets, campus security patrol car computers, and others devices, to provide complete visibility and control, especially for K-12 environments.

Contact us to learn how Faronics can simplify your K-12 environments' IT operations.

Faronics™

www.faronics.com

Faronics' solutions help organizations increase the productivity of existing IT investments and lower IT operating costs. Incorporated in 1996, Faronics has offices in the USA, Canada, and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

CANADA & INTERNATIONAL
1400 - 609 Granville Street
P.O. Box 10362, Pacific Centre
Vancouver,BC,V7Y 1G5
Phone: +1-604-637-3333
Fax: +1-604-637-8188
Email: sales@faronics.com

UNITED STATES
5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA
Call Toll Free: 1-800-943-6422
Fax Toll Free: 1-800-943-6488
Email: sales@faronics.com

EUROPE
8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, England
Phone: +44 (0) 1344 206 414
Email: eurosales@faronics.com

SINGAPORE
20 Cecil Street, #104-01,
Equity Way, Singapore,
049705
Phone: +65 6520 3619
Fax: +65 6722 8634
Email: sales@faronics.com.sg