Transforming the Classroom Experience:

K12 Education Mobility Management Best Practices

Transforming the Classroom Experience:

K12 Education Mobility Management Best Practices

In today's mobile world, the classroom is no longer an environment where students sit and listen to the sage on the stage. With mobility, education becomes an interactive experience. Books and lectures are no longer the sole means to an effective education. A student with a mobile device in hand has access to an endless supply of information.

Students can access supplemental materials, ask for help or begin an assignment, all with a swipe or tap of a finger. In today's classrooms, students are taking learning into their own hands. And teachers are transforming curriculums with personalized instruction and unprecedented access to multimedia materials – ebooks, videos, photos, educational applications and more. Best of all, mobility is helping educators make learning more fun.

Mobile devices provide educators with unique opportunities to improve the learning experience, inside and outside the classroom. However, for all of mobility's benefits, introducing mobile devices into the classroom also presents risks. School IT staff must proactively mitigate those risks in order to maintain regulatory compliance and student privacy and ensure the needs of students, teachers and parents are met.

With AirWatch®, IT administrators can track and manage mobile devices, configure security policies, distribute apps and content, secure access to networks and equip teachers with enhanced device controls, so educators can focus on teaching and students can focus on learning.

The following whitepaper outlines best practices for mobility management in education to help educators embrace the next generation of learning.

Maintain Compliance and Protect Student Information

Schools that are hoping to benefit from the E-rate program – a federally-funded discount for specified communication services and products – must comply with the Children's Internet Protection Act (CIPA). Congress passed CIPA in 2000 to address growing concerns about a child's access to inappropriate content online. According to the Federal Communications Commission (FCC), schools and libraries may not receive the E-rate discounts unless they have appropriate technology protection measures in place.

AirWatch can both set the restrictions that CIPA requires and monitor compliance through the automated compliance engine. If a device breaks compliance, IT can be automatically notified, or AirWatch can automatically perform pre-set escalating actions. Through preconfigured automated policies, the AirWatch compliance engine can automatically send a warning to students that have downloaded unauthorized applications. Administrators can preconfigure escalating actions, which will occur if the student has not removed the application after a specified time period. One school chose to have the compliance engine send an email adding the student's name that broke compliance to that day's detention list.

According to CIPA, schools "must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors)." In addition, meeting CIPA compliance requires schools to adopt and implement safety policies addressing the following:

a. Access by minors to inappropriate matter on the Internet – AirWatch can monitor web traffic and restrict access to specified websites (see below for more details).

b. The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications – In addition to restricting web access, AirWatch can block access to email, apps, and other native chat or messaging functions.

c. Unauthorized access, including so-called "hacking" and other unlawful activities by minors online – The AirWatch compliance engine automatically monitors devices for rooting and jailbreaking attempts and notifies administrators when policies are broken. AirWatch® App Reputation Scanning is also availible along with partnerships with app security software vendors.

d. Unauthorized disclosure, use, and dissemination of personal information regarding minors – A customizable Terms of Use created in the AirWatch console can help IT administrators clearly communicate policies for disclosure, use and dissemination of student information on mobile devices. AirWatch also protects against data loss in a number of ways (see content and application sections below).

e. Measures restricting minors' access to materials harmful to them – AirWatch administrators can block access to content based on app store age rating or by media rating.

Supervision

Supervised mode unlocks additional controls over Apple devices, such as the ability to block access to certain native iPad functionality that cannot be disabled with MDM alone. Some of these functions can help support CIPA compliance. Using supervised mode, administrators can set the following restrictions on an Apple device from the AirWatch console:

- Single App Mode: Locks a device into a single app (ideal for test-taking and shared devices)
- Global Proxy: Allows administrators to force all Internet communications through a single proxy server
- Enable or disable AirDrop: Allows or restricts the transfer of files wirelessly
- Enable or disable iMessage use: Allows administrators to turn on or off messages sent through Apple's Internet-based messaging system
- Enable or disable data usage for apps: Applications can be prevented from using cellular data
- Enable or disable manual profile installations: Allow users to set up their own profiles
- Enable or disable account modification: Allow changes such as altering a user's Apple ID, mail, contacts and calendar

On other device platforms, administrators can set similar restrictions through the AirWatch console to achieve advanced management functionality.

Monitoring Online Activities

Maintaining CIPA compliance will require the ability to monitor students' online activities. With AirWatch® Browser, schools have the ability to enable secure access to specified sites, without the use of a third-party virtual private network (VPN).

AirWatch provided Manitou Springs School District, a public school system in Colorado, the ability to restrict web access. "We wanted to control access to the Internet and turn Safari on and off as needed," says Catherine Butler-Olimb, the district's technology coordinator. AirWatch's multitenant architecture also helped Manitou Springs easily designate levels of Internet access based on grade level. "We also wanted different levels of access for a variety of age groups."

Many schools choose to block access to certain websites, such as Facebook or other social media sites, by blacklisting them in the AirWatch console. For stricter browsing management, administrators can whitelist, or allow access to only pre-approved websites, and block access to all other sites.

With AirWatch® Mobile Device Management, schools can configure policies by using the AirWatch compliance engine to automatically monitor and uphold policies which protect students from inappropriate sites, applications and content.

Digital Citizenship

In 2008, the Federal Communications Commission (FCC) added an amendment to CIPA regarding the education of students about appropriate online behavior. The amendment, titled the Protecting Children in the 21st Century Act, requires schools to educate minors about appropriate online behavior, "including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response."

Setting parameters for appropriate online behavior, or digital citizenship, is a necessary component of education in a mobile environment and can be critical to the success of a school's mobility initiative. Digital citizenship teaches students online etiquette, respect, security measures and laws.

Fredy Padovan, executive director of development and technology at Immaculata-La Salle High School, teaches his students the importance of being a good digital citizen immediately after they receive their school-issued mobile devices. "We've actually started to reconfigure our curriculum. What we've done is started incorporating [digital citizenship] into our freshman computer classes, our freshman critical thinking classes and throughout the curriculum for other courses." Immaculata-La Salle runs a one-to-one iPad initiative, and educators at the school hope to teach students the right values now as they prepare for college and the working world.

"If we are not teaching students how to behave on their devices now, then we aren't doing them any favors," says Padovan, who recognizes that mobile devices will continue to become more integral to business and everyday life. Padovan, an Apple Distinguished Educator, uses **commonsensemedia.org** as a resource for digital citizenship best practices. Padovan notes that digital citizenship is the collective responsibility of everyone involved, including parents, students and educators.

Streamline Staging and Enrollment

Staging and enrollment can be a major hurdle for schools that want to provide their students with mobile devices or initiate a BYOD program. Maintaining compliance with education-related regulations often necessitates the use of MDM on every device. Enrolling all devices in management can be a difficult task for large school systems with multiple locations and limited IT resources.

AirWatch provides a consistent, app-based enrollment flow for all major platforms, and allows both administrators and end users to enroll devices. When users enroll, they are authenticated and the appropriate restrictions, apps and content are pushed automatically.

Josh Hanke is the only IT staff member at St. Andrew's School, an independent K12 school with a one-to-one iPad program. Finding a solution which students could enroll in without the help of IT was critical to the program's success. "I'm a one-man IT department that manages all of our iOS and OS X devices, so I was looking for an EMM partner that was reasonably priced, required minimal effort from faculty and provided a user-friendly interface."

When new students are issued iPads, they are given simple-to-follow instructions to enroll the devices in MDM. "Minimizing the initial setup process will help to reduce the number of students who fail to enroll," Hanke says.

AirWatch offers several methods for staging and enrolling devices that can help streamline the process for educators.

Enrollment through the AirWatch Agent or URL

Administrators can instruct students to navigate to the app store on their devices and download the AirWatch® Agent, which when opened, will prompt users to enter their school credentials to enroll. Students then simply follow a series of prompts, and the device is automatically configured over-the-air (OTA) based on profiles administrators have configured in the AirWatch console. This enrollment method works across device types.

Similarly, administrators can direct students to a URL that will prompt them to enter their school credentials. Browser-based enrollment prompts students to follow steps similar to those required by the AirWatch Agent, only through a browser rather than an app.

Apple Device Enrollment Options

The Device Enrollment Program (DEP) from Apple is having a profound effect on how Apple devices are being deployed and enrolled. DEP provides a seamless process for enrolling devices into MDM by integrating prompts for enrollment into initial device setup. With DEP, devices can be supervised over-the-air (OTA), meaning that they can be configured from a remote location without an administrator having to physically touch the device. For education IT administrators this step can save hours, if not days, of work.

Fredy Padovan, executive director of development and technology at Immaculata-La Salle High School, recently used DEP to stage and enroll 600 new devices in two-and-a-half hours. "My life has been given back to me," says Padovan. "Now, it's just so much easier to get the iPads out the door and get the users configured with all the resources they need."

In addition to decreasing the workload, DEP comes with several other benefits. If a device is enrolled with DEP, administrators now have the ability to disable a student's ability to remove management and configuration profiles. This was not possible prior to DEP.

With DEP, the need for physical staging or provisioning processes can be nearly eliminated. DEP lets students enroll into MDM during the device's activation process. Referred to as zero-touch enrollment, this feature allows administrators to quickly enroll hundreds or thousands of devices at a time. "[The process] was literally just opening up the box and handing the device to the user. It was pretty straight forward," says Padovan.

In addition, with DEP and AirWatch, administrators can skip and customize steps in the device's activation process to ensure all students have the same enrollment workflow. DEP also drastically reduces the number of post-enrollment steps through the use of silent application installations.

For more information, read **The DEP Program Guide from Apple**. Program enrollment instructions are located on the second page.

Apple Configurator is a familiar staging tool for many schools. Configurator helps schools mass enroll and supervise devices. Prior to the introduction of DEP, Configurator was the only way to use supervised mode on an Apple device. Many schools are still using Apple Configurator, which is compatible with AirWatch, to manage their school's iPads.

AirWatch enables administrators to take advantage of OTA updates, mass configuration and remote management. Without AirWatch, a device managed by Apple Configurator requires IT to tether each device to a central Mac to make changes to the device's profiles.

To learn more about Apple Configurator visit Apple's **About** and **Apple Configurator Help** pages.

QR Code Enrollment

QR code enrollment can be a good option for older students. Administrators can email students unique QR codes, which students can scan to enroll in AirWatch management and receive specific content and profiles. Using a QR code generator, administrators can prepare QR codes based on environment URL and group ID. Within the AirWatch Agent, users can select the "QR Config" button to scan the QR image and automatically connect to the correct environment.

Upgrading Devices

Education has been one of the more receptive industries to technology because the tablet has proved to be a powerful learning tool. Many progressive schools are nearing the time when devices need to be upgraded. This can be a difficult and complex process when large numbers of devices and students are involved. There are a lot of moving parts.

Immaculata-La Salle's executive director of advancement and technology offers his advice and lessons learned from his experience. "There isn't a one-size-fits-all deployment workflow," Padavon says. "Test it out, get a work flow that works for you and do it," he suggests. Padovan used groups of seniors to experiment with his collection and enrollment flow before distributing and enrolling 600 new iPads. "I kind of used them as guinea pigs in small groups and kept refining the instructions more each time, until it just became very clear what they needed to do. The process was completely refined."

Padovan drafted simple instructions for his students to follow. His first attempt was a step-by-step guide that included 42 steps. After his tests, he found that only 21 shorts steps are needed.

You can learn more about Immaculata-La Salle's iPad program on their information site **ilsipads.com**. For more information on Padovan's successful deployment workflow, visit **A Fresh Start**.

Manage Multiple Device Ownership Models

Similar to device type or operating system, the ownership model of a deployment will affect the way devices are managed and monitored. AirWatch makes managing different ownership models simple, and administrators can do so from a single web-based console. The AirWatch administrative console shows admins device details, such as ownership type and compliance status. The details can easily be viewed from the console or exported for reporting purposes. Further, AirWatch administrators can sort and search by device type or ownership model and even drill down on individual devices for more information about specific users or devices.

One-to-one

Some schools provide each student with his or her own personal device. A one-to-one initiative, as the approach is often called, allows for the student to save work on the device, take it home and personalize native applications such as iTunes. But as students mature, the device that best suits their needs will also change. For example, tablets are ideal for elementary learning, but more advanced students may require devices with more processing power, such as laptops. AirWatch can manage both.

St. Andrew's School provides iPads to students from K through 10th grade. After their sophomore year, students turn in their iPads for MacBook Air laptops. IT administrator Josh Hanke uses AirWatch to manage and track both student tablets and laptops. Having one central console for all of the devices, both tablet and laptop, "really helps for management and inventory purposes," says Hanke.

Shared Devices

For schools that don't have the budget for a one-to-one tablet or laptop program, the shared device feature from AirWatch can provide a solution that still allows students to use technology in the classroom.

Shared device programs enable students to check devices in and out. Using single app mode, shared devices can be locked into the AirWatch Agent and in order for a student to use the device, he or she must enter their school credentials. When a student finishes using the device and checks it back in, the device will revert back to its original, unassigned state. For example, a school may have 30 shared devices for each classroom. The devices stay in the same classroom, but as the students switch from class to class they are able to log into several different devices throughout the day with the same user credentials to access a device configuration that is specific to them.

BYOD

In rare cases, K12 schools have implemented a "bring your own device" (BYOD) policy. This type of deployment is more common in higher education.

For BYOD deployments, AirWatch has the ability to assign different restrictions on the device based on whether the student is at school or at home. AirWatch administrators can create a virtual perimeter around the school called a geofence. When students are inside the perimeter, their devices are subject to the restrictions the school administrator has set. For example, an administrator can restrict certain gaming apps or the device's camera when a student enters the geofence. When the student leaves, the device regains full functionality and the student can use the device in the exact same way they normally would.

Enable Content Sharing and Collaboration

One of the greatest advantages of a mobile device is that it gives students the ability to share and collaborate on assignments. Projects, tests, quizzes and papers can all be distributed, completed, shared, amended and graded from a mobile device. With a tablet, teachers can distribute learning materials quickly and easily, based on class or an individual student's needs.

AirWatch® Secure Content Locker™ is a mobile content management solution that enables students to securely access, share and collaborate on files with their mobile devices. Secure Content Locker, which can be used with AirWatch Mobile Device Management or as a standalone app, creates an encrypted container on the device that can store content or provide access to existing file repositories. Secure Content Locker gives students the ability to edit and share documents as easily as they could from a desktop computer, ideal for working on group projects on the fly. Teachers can use Secure Content Locker to distribute assignments, and students can turn completed work back into the teacher by dropping documents into the teacher's private file repository. Teachers can also comment on or grade student work from within the app.

AirWatch administrators, including teachers that have been designated as content administrators, can also push content to specified devices from the AirWatch console. For example, school-wide announcements can be sent to everyone with Secure Content Locker installed. On the other hand, if a document needs to be sent only to staff or a specific class or grade, administrators can select just the group intended to receive the document. Teachers can even send supplemental materials solely to individuals who may need extra help.

AirWatch Secure Content Locker helps protect against data loss and maintain compliance. For example, administrators can restrict the opening of email attachments to AirWatch Secure Content Locker for the opening of hyperlinks within documents to AirWatch Browser. This helps to ensure sensitive content never leaves an encrypted space and limits the threat of a malicious attack.

Manage Applications

With AirWatch, administrators can manage the entire application lifecycle, from initial testing through deployment, updates and retirement. Administrators and even developers can test applications in AirWatch through a controlled release, which enables deployment to a control group of students or staff to test for issues before widely deploying the app. AirWatch offers application versioning, which enables IT administrators to require application updates – this can be done organization-wide or through a phased rollout.

Schools can make both public and custom applications available to users through the AirWatch® App Catalog, a customizable app catalog that only students and staff can access. Immaculata-La Salle makes several education-specific apps available through a custom app catalog. The school is moving towards a paperless classroom with apps such as **Showbie**, **Turnitin** and **Nearpod**.

The school is even letting students take an active role in the selection of applications for their schools app catalog. Administrators can test and approve apps from the AirWatch console and deploy them simultaneously to specified student or faculty devices. AirWatch enables distribution of apps based on smart groups that can be categorized by location, class or other variables.

App Restrictions and Security

AirWatch® App Wrapping allows schools to secure their apps from malicious attacks or other security vulnerabilities. Administrators can simply wrap the application from the AirWatch console and AirWatch security features are added to the application.

AirWatch also enables IT administrators to remove access to a device's native app store, which prevents students from downloading unsanctioned applications.

For some schools, it may not be necessary to block the device's native app store. However, in order to reach CIPA certification, schools will need to deny access to specific applications which may expose students to inappropriate content or distractions. With AirWatch this can be done by whitelisting or blacklisting applications.

IT administrators can whitelist applications to approve them for students and staff. A whitelist disables the ability to download an application not on the whitelist. A blacklist denies access to only the applications that a specifically placed on the blacklist.

Volume App Licensing Programs

AirWatch enables the use of all major app stores' volume licensing programs, which provide educators discounts when they buy apps in bulk. This prevents students from having to register devices with their purchasing information or IDs. Schools can pay for bulk purchases and then distribute single licenses to devices OTA. Once a license has been distributed, students can be prompted to download paid apps without having to enter payment information.

AirWatch supports volume purchase and distribution through the following programs:

- **Google Play for Education**
- **Apple Volume Purchase Program**
- **Microsoft Academic Volume Licensing** (coming soon)

Enable Faculty

AirWatch recognizes that the introduction of mobile technology into the classroom represents a tectonic shift in the way teachers and students interact. While it opens many doors for new forms of education, it also introduces new complexities and potential distractions from the teacher at the head of the class.

AirWatch has developed a set of apps for teachers and students that are specially designed to ensure teachers maintain control over a connected classroom. The AirWatch® Teach app provides a simplified management portal where teachers can closely manage devices in their classroom without having to call IT.

With AirWatch Teach, teachers have access to simple management tools such as:

- Single App Mode: Teachers can lock a device into a single application or website at will or for a specified period of time. This can be useful for test-taking or ensuring students stay on task during assignments.
- Transfer Files: Teachers can easily send and receive files, such as ebooks, by transferring over Bluetooth or Wi-Fi.
- Reset Passcode: Teachers can instantly reset and recreate the passcode when students forget, rather than having to call the IT helpdesk and wait for a response.
- All Eyes Up Front: With the swipe of a finger, a teacher can simultaneously lock students' devices to bring their focus back to their teacher and away from their device. All Eyes Up Front also provides some interesting uses outside just keeping students focused. For example, during a timed quiz or test, the teacher can use All Eyes Up Front to lock the device once the time-limit has been reached.

"I'm foaming at the mouth to get my hands on Teacher Tools," says Immaculata-La Salle's Executive Director of Development and Technology Freddy Padovan. "The teachers keep asking me for it, because I've shown them the demo video on YouTube. After I showed them the first feature there was applause in the room."

Group Devices and Applications for Simplified Management

With AirWatch, schools can take advantage of organization groups for multitenant device configuration and management or smart groups for pushing content and applications. Organization groups help IT administrators categorize students by school, grade or class.

Organization Groups

Organization groups are one of the first things an AirWatch administrator will create when setting up management for a fleet of mobile devices. Administrators can organize their deployment into large groups, such as grade level, faculty or school district. At St. Andrew's School, Director of Technology Josh Hanke creates organization groups for each grade level. Then, rather than configuring each device, Hanke can create a single profile for each grade level that he can then apply to all devices in that group. Profiles can become less strict as students advance. Each year, Hanke adds a group for incoming students and deletes the organization group containing students that have graduated, a process which he says requires minimal work and helps automate the configuration of management profiles.

Smart Groups

AirWatch smart groups can simplify the grouping process. Smart groups are custom groups of devices that administrators can define for application, profile, or content assignment. Administrators can create logical smart groups based on a number of criteria, including ownership type, device platform, user group, model and operating system (OS). Administrators can configure smart groups that apply to a group of specific devices and/or users, and devices and users can belong to multiple smart groups.

Once defined, administrators can reuse smart groups for assignment to any applications. Multiple smart groups can be assigned to a single application. This feature is useful for fine-tuning who should receive certain apps. For instance, students in AP classes may require different apps. Administrators can create a smart

group for those students and deploy applications only to those students.

Hanke uses smart groups to get more granular with app distribution. "Now, I can send apps to individual students or to smaller groups," says Hanke. If a certain teacher wants a certain class to have access to an app, but not the entire grade level, Hanke says he can go into the AirWatch console and create a smart group just for that class.

Location-based Grouping

Large deployments across multiple campuses may want to apply unique configurations and different content to devices based on the school where they are ultimately used. In order to simplify the process of staging enrollment for numerous devices, schools can leverage network range assignments to provision devices based on their IP address. With this method, administrators don't have to worry about the assignment group of the original enrollment user because devices will be re-assigned based on the network range from which they report back to AirWatch.

Existing Active Directory (AD) users that reside in different user groups based on location can use existing AD credentials. For basic users without AD credentials, administrators should ensure they reside in different organization groups to receive different configurations. Administrators then simply define the process to stage enrollment for numerous devices. Devices are then shipped to their various locations or stores, and once the devices check in from their new Network Ranges, they will be re-assigned to the users defined above, and configured with the associated settings.

Preparing School Networks

AirWatch recommends setting up a secured Wi-Fi network for students and faculty and a public network for visitors. Within the AirWatch console, administrators can limit Wi-Fi connection on managed devices to the secured network, so devices with access to student information cannot access the public Wi-Fi network.

To ensure the security of the private network, AirWatch partners with several leading network access control providers. Network access control can detect any new or unmanaged devices that attempt to join the secure network and redirect them to the AirWatch Agent or enrollment URL to enroll (or re-enroll) a device. This ensures that the IT administrator has oversight for all devices accessing the secure network.

Track Assets from a Central Location

A critical aspect for a large school deployment is the ability to manage and track devices remotely in real time. Through the AirWatch administrative console, administrators can manage an entire fleet of devices, configure settings and distribute applications and content without ever having to physically touch the device.

The central management console helps administrators see which devices are out of compliance, when the devices last checked in with AirWatch and what applications are on the device, regardless of device type or OS. If a device is reported as lost or stolen, administrators can wipe all sensitive information from the device, with a single click in the administrative console.

But mobile devices go beyond smartphones and tablets. School administrators need a simple way to deploy, secure and manage all devices, including smartphones, tablets, desktops, laptops, netbooks and notebooks. With AirWatch, administrators can manage all of these devices from a central location.

Additional Resources

For additional information, visit:
www.air-watch.com/industries/education

To get started with a free trial of AirWatch, visit **www.air-watch.com/free-trial**.

AirWatch Global Headquarters

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch by VMware

AirWatch by VMware is the leader in enterprise mobility management, with more than 12,000 global customers.The AirWatch platform includes industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at **www.air-watch.com**.