

Mobility management in the Classroom - Best practices

WHITE PAPER

hexnode

Table of Contents

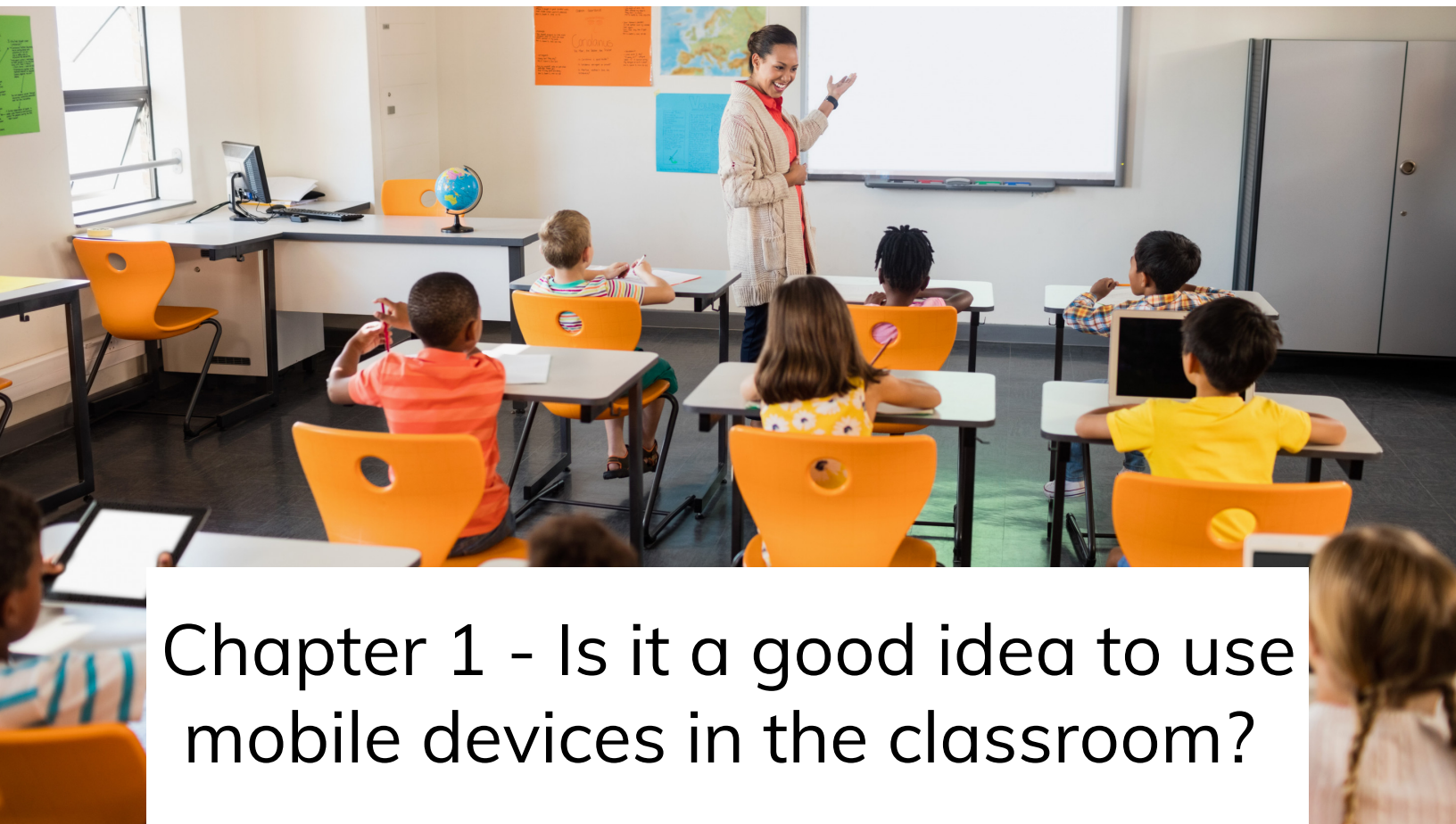
Growth of mobile devices in the classroom	03
Chapter 1: Is it a good idea to use mobile devices in the classroom?	04
Benefits	04
Disadvantages	05
Chapter 2: Role of EMM – What it does and how it benefits schools	06
EMM for schools	08
Chapter 3: How to pick the right EMM for your school?	13
Best practices to facilitate mobility in the classrooms - Our take	14
Key considerations towards choosing the right management tool	14
Implement the best management practices to help students get a better learning experience	16
Chapter 4: Leveraging Hexnode to deliver unique learning experiences	22
Automated enrollment and over-the-air content deployment	23
App management	23
Remote management	24
Security management	24
Containerization	25
Device lockdown	25

A photograph showing a female teacher with long brown hair leaning over a group of young students in a classroom. They are gathered around a table, looking at and interacting with several tablets. The tablets display various educational content, including math problems and colorful charts. The background shows bookshelves filled with books.

Growth of mobile devices in the classroom

Mobile learning has accelerated with the increased use of smartphones and tablets in the classroom. The old days of rote learning and listlessly listening to teachers are increasingly being obsolete. With the advent of technology, most students who belong to Gen Z want their learning experience to be more fun and interactive. They don't remember a time when there was no internet and so it makes sense why schools should start adapting mobile devices within their classrooms to enhance the learning experience of their students. Mobile learning is always an issue where people stand divided, while most believe that if schools adopt strict device usage policies it can help students remember their lessons well and also encourage them to develop several skills along the way. While, others feel mobile devices can only inhibit the learning process by being a distraction to students.

Nevertheless, the usage of mobile devices continues to be well adapted by many schools as it provides students with the flexibility to write entire essays on their smartphones and complete their assignments on the bus. Instead of referring to just dense texts, students can now write more interactive essays and easily accessible reference links from textbooks online. This mode of learning can be beneficial for teachers too as it provides them with quick access to the resources they need and the various tools which help them boost up the learning process of their students.



Chapter 1 - Is it a good idea to use mobile devices in the classroom?

The use of mobile devices within the classroom has always been an intensely debated one. Despite the benefits they bring and having clear rules set on their usage, some teachers still feel that smartphones and tablets will distract students from their studies. There will always be that lingering worry that these devices could also be used as tools for cyberbullying. Before your school makes a decision on whether it would be feasible to deploy mobile devices to students, it's always a good idea to look ahead and have a clear picture of what this would entail:

Benefits

- Students can have instant access to the information they need.
- Teachers can create interactive contents to improve the cognitive ability of the students.
- Better interaction between the students would make the learning process more fun and keep them from getting bored.
- Mobile devices can promote the concept of learning from anywhere. Students can learn outside of their classrooms. The pandemic has made e-learning more of a necessity than a choice.

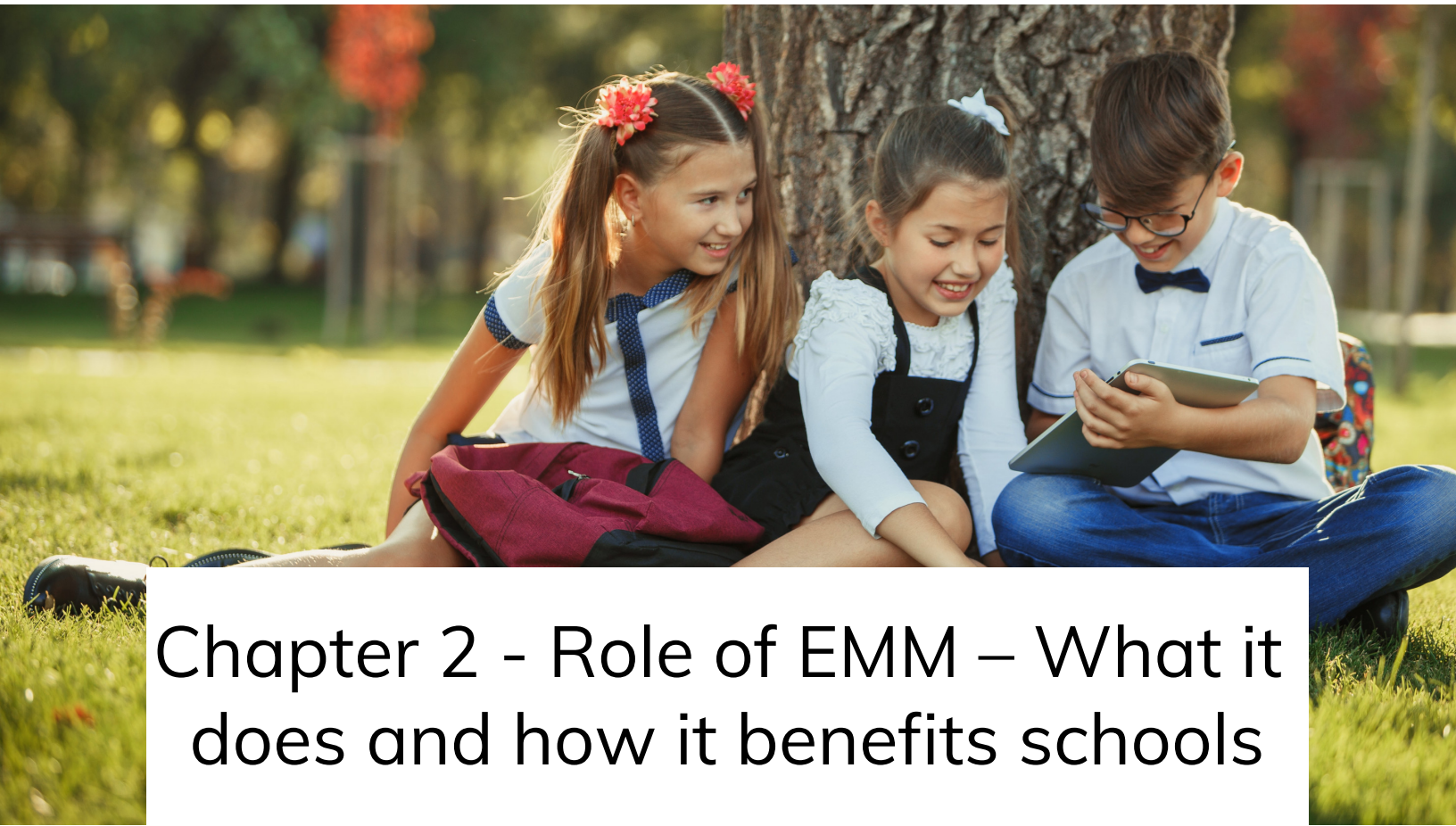
- Educational apps installed on these devices can help students keep track of the progress of their studies. Teachers can install apps to evaluate the performance of their students.
- Teachers can collaborate with their students and assist them more efficiently.
- Shared devices can help improve communication among students.
- Mobile learning will give older students the freedom to be more flexible in their studies and develop their time management and productivity skills.
- Students will always prefer a learning approach that is convenient and efficient, both in terms of their needs and time, this can be easily achievable through mobile devices.
- Mobile devices can help bridge the gap between parents and their children, where parents can get an insight into their classroom activities and pending assignments.
- Mobile learning can help prepare students for the future, where e-learning will be a common approach adopted by businesses to train their employees.



Disadvantages



- Students may face distraction from their learning activities, they may waste time surfing the internet or social media.
- Mobile devices can be used as tools for cyberbullying where harmful content about fellow classmates can be posted online.
- Bringing these devices to schools can increase the risk of theft.
- Students may look up answers during tests.
- Various security issues may arise.
- Schools will have to spend more on network connections since they have to support the student devices as well.
- Securing the devices may add up the daily chores of the school management.



Chapter 2 - Role of EMM – What it does and how it benefits schools

With Enterprise Mobility Management (EMM), admins can easily oversee mobile devices used within their schools. EMM is a collection of various other management tools such as Mobile Device Management (MDM), Mobile Application Management (MAM), Containerization, Mobile Content Management (MCM), Mobile Expense Management (MEM), Mobile Security Management (MSM), and Identity and Access Management (IAM). In order to maintain the productivity of your students and maximize the security of the deployed devices, always consider going for an EMM solution that offers all of the above. Device management terms are often used interchangeably even though they have distinctive features of their own. Here is a list of what each facet of EMM offers to institutions that use them:

Mobile Device Management (MDM): helps admins to manage mobile devices through their entire lifecycle. It involves the installation of profiles that gives institutions the ability to control and enforce various security policies onto the user end devices. Data can be remotely wiped from the device if it gets reported lost or stolen. MDM can also help admins to enforce strong passwords and track the location of the devices. Devices running on outdated OS versions will always be an open gateway for hackers to mine

confidential information. With MDM, OS updates can be remotely pushed onto the devices and keep them safe from various vulnerabilities. This is a handy part of EMM that helps admins to keep track of their device inventory.



Mobile Application Management (MAM): calls for the easier management of the applications. With MAM, all the applications needed by your school can be installed with minimal to no user interference. The apps can also be updated and their licenses managed. Specific settings can be configured onto the applications and they can be selectively removed from a single device by means of pushing a policy that calls for the uninstallation of that particular application.

Containerization: has its own importance although considered as a part of MAM. Containerization facilitates the separation of learning data from personal data and helps protect user privacy without compromising the school's security.

Mobile Content Management (MCM): help teachers and students get instant access to the study materials they need at the moment. Content management also provides your school with an extra layer of security that ensures only authorized users have access to the contents that are being pushed onto the devices.

Mobile Expense Management (MEM): is an important part of EMM that helps admins to keep track of the costs and network usage. Once students start using school deployed or personal mobile devices on a more regular basis in the classroom, schools will have to start spending more on network connections. To curb the oncoming network expenses and ensure that no data hogging happens, it's always wise to have a mobile expense management strategy in place.

Mobile Security Management (MSM): protects the endpoints and confidential data in an organization. Enterprise data is protected with encryption of data at rest, in use and in motion. Device and application-level security is achieved by enforcing network restrictions, app usage control, etc.

Identity and Access Management (IAM): help schools ensure that only authorized users have access to their data and applications. IAM includes the use of authentication and single sign on. This helps schools and other institutions to keep a proper track of the devices and assign departmental wise usage of applications.

EMM for schools

Here are some of the benefits schools can experience by bringing EMM on board:

Single sign-on

Single sign-on offers the advantage of verifying users and providing them with the convenience to use just a single username and password to access the resources that they need. This will free your school from storing passwords within their databases and cut short any troubleshooting issues that may arise from logging in. When your users log in to a particular website via Single sign-on, the website checks with a Single sign-on provider such as Microsoft, Google, or Okta to verify the user's identity. Schools can integrate with directory services like Microsoft Active Directory and Azure Active Directory to ensure that access to applications and various other resources is done in a secured manner.



Benefits:

- It saves users the trouble of remembering multiple passwords, single sign-on offers them the convenience to use just a single set of login credentials.
- Microsoft, Google, and Okta are brands that come with a sense of trust, new users can sign in without feeling uneasy.
- It helps reduce risks that come from users implementing bad password habits.
- Single sign-on coupled with 2FA gives your school's network an extra layer of security.

Manage users

Managing users within your school without EMM can be a hefty task. EMM provides IT admins the flexibility to easily create new users and apply several remote actions to manage the devices of existing users.

Benefits:

- Onboard new users more quickly by sending bulk enrollment requests.



- View user details to check whether their devices are enrolled and compliant with all the deployed policies.
- Create user groups by grouping users that have a common attribute such as grades, department, device type, or OS.
- Manage the user end devices efficiently by utilizing various group management functions such as clearing passcodes, initiating a device wipe, associating policies, locking lost devices, and scanning the device location to ensure the safety of the device and to keep track of the device inventory.

Deploy and manage relevant applications

App management is an integral part of school environments to function smoothly. Any application needed by the teacher can be remotely pushed onto the devices. You can ensure security by having the apps updated to their latest version, while some admins may prefer not to upgrade, it's always better to do so as it may save you the trouble of dealing with various vulnerabilities in the future.



Benefits:

- EMM's that integrate with Apple's Volume Purchase Program helps schools to easily purchase the required applications in bulk, deploy and manage them.
- Get an extensive app management capability with remote installs, uninstalls, and upgrade it to ensure app security.
- Whitelist applications to boost productivity among students.
- Blacklist applications to remove all distractions and minimize the occurrence of cyberbullying.
- Set in-app configurations, permissions, and approvals.
- Set important apps as mandatory and ensure that students have them installed on their devices.
- Create app catalogs with the required apps, push them to the devices by associating it as a policy.
- Create containers on the personal devices of students to maintain a clear distinction between the school apps and the personal apps of the students.
- Create app groups to push multiple apps to a single user or multiple users.
- Manage app licenses.

Lock down devices to ensure students stay focused on their studies

One of the challenges in bringing mobile devices into the classroom is the ever-present worry that students may get distracted from their learning activities. While this may be true, admins can prevent this to a large extent by locking down the devices to function with just the essential applications during school hours. This would be extremely useful during tests when students need to be prevented from looking up answers. By locking down the devices to a kiosk mode, admins can ensure that students don't tamper with any of the device's settings. You can even whitelist an application and keep it hidden from users by setting it as a background app.



Benefits:

- Configure the peripheral settings to get more control over the managed devices.
- Set background apps that are needed but cannot be directly accessed by the user.
- Lock the devices into a single app or multi app kiosk mode.
- Lock down devices running on iOS into an autonomous single app mode, where the whitelisted application running in the foreground will exit itself once its functionality is over.

Minimize the occurrence of data breach

All data that passes in and out of the school's network can be safeguarded by deploying several data loss prevention policies. With the help of EMM, admins can ensure that any confidential information be it the student's personal information or school records stay within the confines of the managed devices and does not fall under the purview of any unauthorized users.

Benefits:

- Deploy policies that prevent managed apps to be opened from unauthorized sources.
- Prevent students from unintentionally sharing confidential information by setting up restrictions on Bluetooth, USB, or tethering.
- Configure the Wi-Fi and VPN settings.
- Enforce a copy/paste restriction on BYO devices.

Deploy the right files and other study materials

Having a good content management system in place is important as it provides both students and teachers with instant access to the resources they need to complete their assignments or work on time.

Benefits:

- Create and distribute contents to multiple devices with ease.
- Easier collaboration among students.
- Restrict the sharing of contents.
- Specify the path of the content so that the files can be pushed within the right folder.



Secure data stored on lost devices

One of the biggest advantages of bringing an EMM on board is it enhances the security of devices in a way that even if a device gets reported as being lost or stolen, admins would not have to scramble about to secure the data present within it. Through EMM admins can quickly initiate a device wipe remotely to ensure that none of the confidential information falls into the wrong hands.

Benefits:

- Scan the device location to get updates on where the lost device is located.
- Initiate a device wipe to ensure the safety of the information present inside.
- Enable lost mode and set up a custom lock screen message to inform the potential finder on where or the whom the device needs to be returned to.
- Set up remote ring.

Get updates on device location

Scanning the device location does not only come handy in situations where you need to track down a lost device. It would also help admins and other school representatives to check whether students who have taken these devices home reach their homes safely.

Benefits:

- Track device location.
- Generate location history reports.
- Do a complete wipe on lost devices.

- Scan device location real time or at periodic intervals.

Enforce strong passcodes

Weak passcodes are the best gateway for hackers to latch on to school networks and mine any of the information they require for personal or financial gain. Thus, it's vital for admins to enforce strong passcode policies on the devices and have users update their passcodes at regular intervals.



Benefits:

- Define the passcode criteria to make it more complex.
- Set the time period in which the passcode will expire.
- Set up passcode history to dissuade users from repeating the same passcodes.
- Define the number of failed attempts, after which the data present within the devices will be wiped.
- Scan device location real time or at periodic intervals.



Chapter 3 - How to pick the right EMM for your school?

As the adoption of mobility in classrooms is changing the fundamental theories of traditional learning bringing tangible values to student efficiency, digital learning will no longer remain in the prototype stage. We've already seen a good deal of endpoints creeping into some classroom environments, and the process is primed to conquer the entire education sector. It's just a matter of time until we see a major explosion of learning devices into the mainstream of education. However, accommodating mobility in the classrooms is not always simple and painless as it's sometimes made out to be. The adoption can either elevate or mitigate the management pain points according to the IT team's efficiency to implement it. A proper strategy should be required to integrate customized learning into the existing systems. Choosing the right EMM is the key to providing a commonplace solution for the management concerns related to this adoption.

Best practices to facilitate mobility in the classrooms - Our take

- Teachers should get acquainted with the new technologies and instruct students on proper device usage.
- Deliver the necessary resources for learning.
- Keep students engaged while maintaining their focus on studies.
- Ensure proper security.
- Choose the right management tool.



Key considerations towards choosing the right management tool



- **Evaluate your requirements**

Which EMM works well for your school highly depends on your particular requirements. So, before deciding on your EMM solution, thoroughly understand what your school is looking to address. Check which all OS platforms you have to support and what kind of devices your students are using. Also, check for all the specific management features that may come in handy for your team.

- **Decide between cloud and on-premises**

Another critical decision to make is to choose between the cloud and on-premises offerings. Most schools opt for cloud-based EMM as they don't have to support any additional infrastructure and maintain them on-premises. But both the services have their own perks and hence are viable options to make.

- **Check whether the EMM solution meet all your requirements**

Some EMMs may not be having support for all the features you need. So, go for the one which solves your pressing and challenging problems in the most effective manner. Some EMMs offer a product trial so that you can explore their features before deciding on the purchase. Find out what all management policies and restrictions can be enforced using the EMM solution.

- **Make sure that the EMM solution is not complicated**

Choose an EMM solution that doesn't require much IT knowledge for device deployment and day-to-day management. The UI should be simple, intuitive and user friendly. All the features should be easy to understand, and the management process should be simple.



- **Ensure that the EMM solution automates most management tasks**
Look for an EMM that can automate the management tasks for your school. The EMM should provide bulk deployment options and make all the possible tasks handsfree.
- **Test your education app's compatibility with the EMM**
Check whether your education apps work well with the EMM solution. Go for an EMM which supports over-the-air distribution and update the apps needed for the students.
- **Remember to check for user level and group wise management options**
User management is a crucial aspect to consider when you decide on the EMM solution. You may have to manage the students, teachers, and other school faculties. All of them have different tasks to complete, and hence their devices are to be handled differently. So, the EMM should allow grouping of the users as well as devices and group wise enforcement of management policies.
- **Look at the EMMs integration with Apple School Manager**
Ensure that the EMM solution integrates well with education management services like Apple School Manager. Such offerings from popular vendors make it even easier to manage your endpoints.
- **Don't forget to look for security**
Make sure that the EMM solution provides adequate security features to take care of the student devices. Be sure to check whether the EMM solution relinquishes confidential data to third parties.
- **Be certain to check for remote management features**
The ability to manage devices remotely is vital in ensuring that the devices and data are always protected wherever they are. Especially in the current global pandemic scenario, both students and teachers may be at home, students attending the class online. In such situations, only an EMM solution with remote management support can help schools keep things going without flaws.

Implement the best management practices to help students get a better learning experience

By relying on a device management solution like Hexnode, schools can easily deploy devices over the air, set necessary configurations, manage apps, roll out OS updates, push security and other data loss prevention policies, do compliance checks, remotely manage the devices and initiate a secure wipe on lost devices. Here's what you need to remember to ensure students get the most out of using mobile devices in the classroom.



Get devices ready



Configure
security settings



Onboard users



Distribute content



Manage

Easily onboard the devices with hands free enrollment options



Hexnode's integration with Apple School Manager (ASM) offers a more simplified deployment experience. With Device Enrollment Program (DEP), the devices can be made readily available to users by enrolling the devices with minimal setup assistant screens. Even if a user initiates a factory reset on the DEP enrolled device, the devices will still remain managed.

Onboarding bulk Android devices with Android Zero Touch Enrollment (ZTE) and Samsung KME, Windows devices via Windows Autopilot will save admins many hours from manually enrolling each device. Hexnode also has integrations with Azure AD, Active Directory, GSuite and Okta, making it easier for admins to sync user and user groups and let users enroll their devices with Hexnode by logging in with their own credentials. However, going for authenticated enrollment may leave some dependency on users. If you need a complete hands-free enrollment, its best to enroll the devices either through DEP or ZTE.

Set restrictions to protect student information

Adopting lax security measures to guard your school networks would be a risky thing to do since hackers will always be on the lookout to spot any vulnerabilities within the networks. Manually handing out the Wi-Fi passwords to students wouldn't be a good idea either as they may unintentionally share them with unauthorized parties. With Hexnode admins can configure the Wi-Fi settings to ensure that devices automatically connect with the school's Wi-Fi network without prompting users to enter the password. You can also configure the VPN settings to ensure that any information shared by teachers and students passes through a private network. Hexnode also provides the convenience to set different security restrictions on the devices to make sure that all confidential data stays within the confines of the school networks and does not stray anywhere else.



Use dynamic groups to automate tasks



One of the greatest advantages dynamic group provides is automation. Dynamic groups unlike custom groups are not fixed. The movement of devices in and out of a dynamic group will depend on whether they meet the criteria. You don't have to manually add a device into the group instead if it meets certain criteria that the admin has set, it will be automatically added to the group. Admins can create device groups and push relevant grade specific applications onto the devices. This saves your faculty plenty of hours to have their requested applications deployed onto the students' devices. Dynamic groups can be used for smoother enrollment, location tracking, and scheduling reports.

Supervise iOS devices to get more granular control

With supervision admins can have more control over the iOS devices they manage such as setting additional restrictions, silent app installations, web content filtering, locking down devices in a Kiosk mode, and sending out custom lock screen messages on lost devices. Devices can be set up as supervised only prior to activation in a new device or a fully erased one. Admins can supervise the iOS devices using either Apple Configurator 2 or DEP. By making the devices supervised, you can monitor the devices even better and secure them from data breaches.



Use web content filtering to block access to websites that contain violent content

Though the internet is a great tool for students to develop their research skills and complete their assignments on time, unfiltered access to it can leave them exposed to a variety of harmful content that may harbor hate speeches and other violent messages. With Hexnode's web content filtering feature, admins can easily blacklist websites that are not only offensive but also block those that can be used by students to perpetuate cyberbullying. Web content filtering should be done in a way that doesn't limit the freedom of students. Before a particular website is blocked, it would be a good idea for school authorities to have a meeting with the students to explain their reasons why that website needs to be blocked. Admins can also whitelist necessary websites and lock down the devices with it to ensure students make the most out of their interactive learning experience.

Lockdown the devices to just the essential apps and websites

Only a handful of apps is needed to make learning fun. As the range of applications and functionalities the students have access to increases, so does the opportunity for malicious activities, breaches, and vulnerabilities. So, providing only what's necessary is an ideal step towards strategically enhancing data security, preventing disruptive behavior from students, and warding off any possible cyber threats. The student devices can be locked down to one or a few applications and websites using kiosk mode. This prevents students from tampering out with what is not meant for them and helps utilize their study time more systematically.

Use the Hexnode kiosk browser to get a more secure and personalized browsing experience

Cybersecurity is a paramount concern when we equip students with learning gadgets and grant them unlimited data to browse for any resources by themselves. Kids may not be efficient in identifying the suspicious things they across the web. So, the better plan is to provide them a secure browser to surf the web. Hexnode provides a secure kiosk browser with which we can blacklist unnecessary websites and allow only what's required for the students. There are many advanced features to customize the browsing experience for them to make learning even more enjoyable.



Use application control features

While incorporating mobility into their lesson plans, teachers should also ensure that the classroom environment is always under control during school hours. The status of learning apps should always be monitored to make sure that the students are never removing anything important from their gadgets. Along with securing the learning apps allotted to the student devices, they should be prevented from downloading or installing inappropriate content.

Monitor the devices for rooting and jailbreaking attempts



Children nowadays are smarter than adults and may be clever enough to root their devices bypassing management and getting into what they actually want to. From a security perspective, rooting is not encouraged on devices as it ultimately breakdown all the inbuilt security features. So, it's essential to detect if any such jailbreaking attempt is occurring with a student device.

Maintain compliance, get notified when a device breaks compliance

The EMM portal showcases the compliance status of all the enrolled devices and

and helps to easily identify if any device remains non-compliant with the management policies enforced by the school. Schools can set to get notified when any of the student devices break compliance. The device's activity status can also be monitored, and the school can do necessary actions if a student's device remains inactive for a long time. Schools, if they want to, can also initiate a device scan on demand to check the real-time activity status of a device.



Secure the devices in a way that even if a device gets lost, it doesn't compromise the data

Kids may not always be careful enough to secure their devices when they are outside the school premises. There are high chances for the device to get misplaced, lost, or stolen and end up in the wrong hands. With MDM, we can manage to secure the data in such situations and make sure that any sensitive data on the device is never compromised at any cost. At first, we can track the geographical location of the device from the EMM, and as an added protection to the data, we can initiate a remote lock or wipe and set the device to the lost mode.

Set up location tracking and monitor the devices



Knowing the real time location of the device is really important when the devices are outside and when students are attending their classes online. This helps make sure that their studies are not compromised along with giving the school confidence that even if the device is lost, they have the provision to either track it by themselves or submit the location history to the authorities to speed up the recovery process.

Have a sound content management system in place to keep track of the study materials

Mobility in classrooms literally means unlimited resources. EMM provides an efficient way to realize this. With EMM, resources can be easily distributed and managed. Schools can enforce content to student devices and check whether the students are removing any necessary study materials from the device afterward.

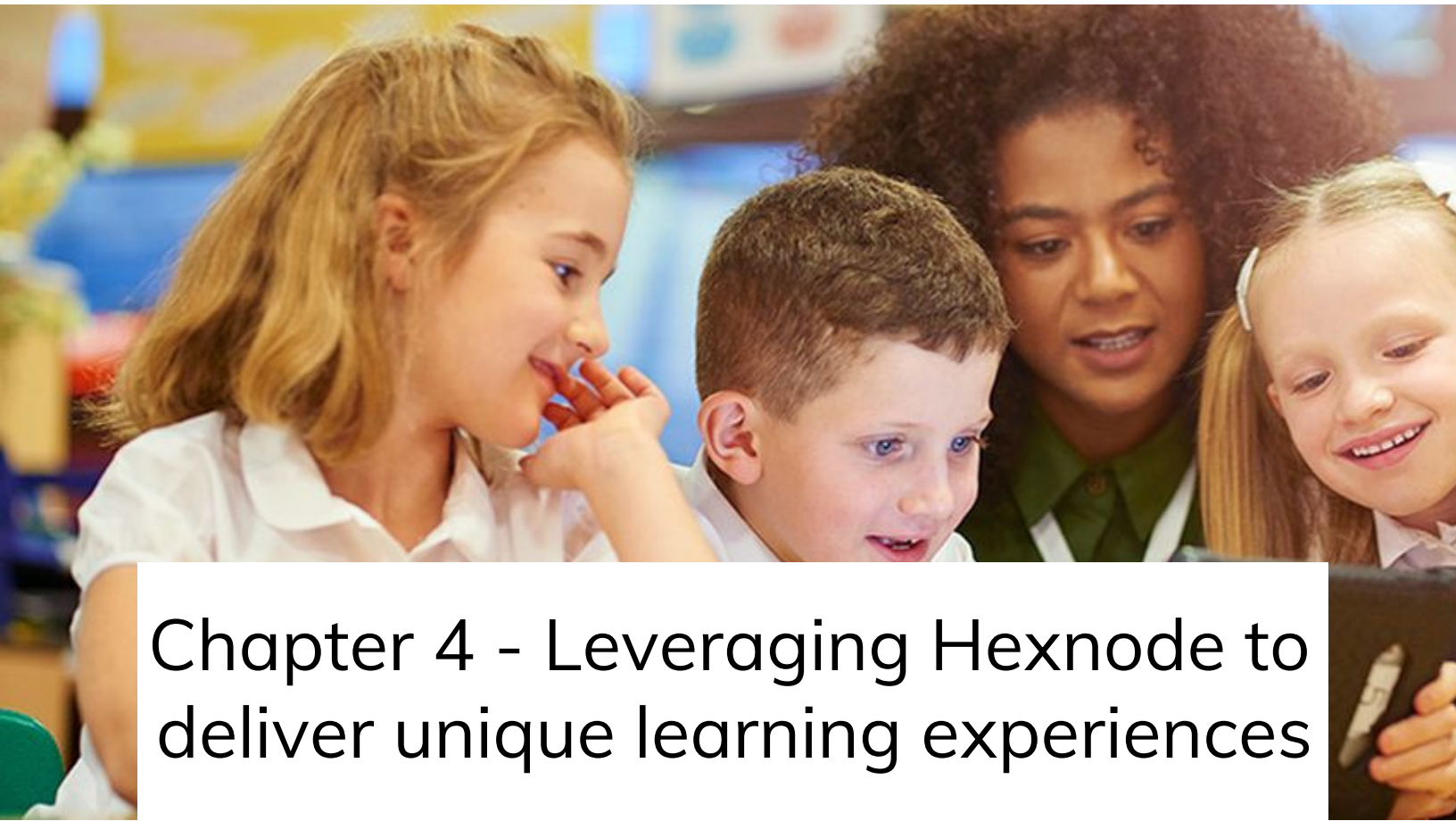
Use Hexnode messenger to help teachers communicate with their students more freely

When learning goes out of the classroom, establishing efficient communication and collaboration is really important. Hexnode provides a messaging tool that helps teachers easily engage with students and give them proper instructions. Students, in turn, can convey to teachers all their concerns related to studies. The Hexnode Messenger works well even when the device is locked down to a purpose specific kiosk mode.



Integrate with Apple School Manager

Apple School Manager integration eases the onboarding, content distribution, and ongoing management process for Apple devices. It facilitates out-of-the-box enrollment, streamlined device set up, bulk content purchase and distribution, on-demand reassigning of apps and books to different users, and many other customizations.

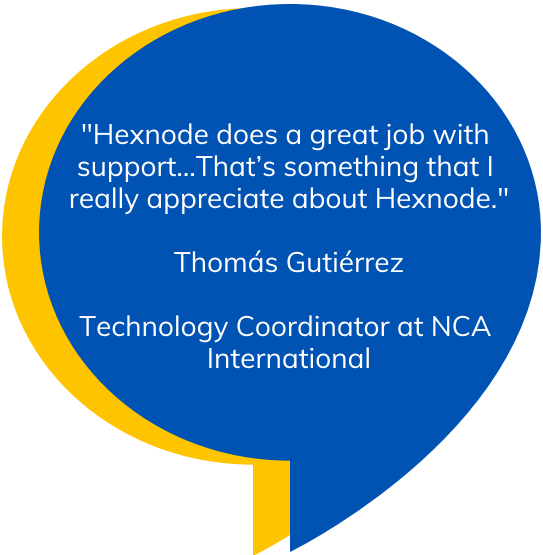


Chapter 4 - Leveraging Hexnode to deliver unique learning experiences

Creating and establishing an excited community in a heavily regulated niche was never easy. Hexnode has always been ready to take a step backward to look at the big picture and offer a diverse stack of management attributes to many educational institutions to deliver an effective digital student engagement strategy. Our customers, not just from the education zone, but across all industrial verticals, find the technical support the team provides really appreciable, to the point that today asking for support is more or less like texting a friend for our customers. Here, we'll take a look through some of the features for classroom mobility management to get a feel for what we offer.

Automated enrollment and over-the-air content deployment

- Integrating with no-touch enrollment programs like Apple School Manager, Android Zero Touch Enrollment, Samsung KME, and Windows Autopilot, EMM provide options to enroll the devices over the air. EMM provides a hand full of bulk deployment options too.
- All the necessary content can be purchased via the ASM portal and silently pushed to the student's devices that are enrolled with EMM.
- App licenses can be retrieved from devices for which the apps are no longer required.



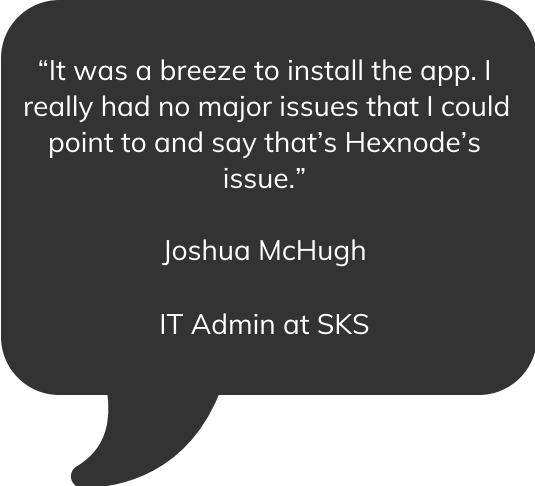
"Hexnode does a great job with support...That's something that I really appreciate about Hexnode."

Thomás Gutiérrez

Technology Coordinator at NCA International

App management

- Essential education apps and learning games can effortlessly be pushed to the student devices in bulk.
- Applications could be installed onto the devices with little to no user intervention.
- Undesirable apps can be blocked, and the students can be restricted from installing anything unproductive.
- Both store apps and in-house apps can be easily deployed.
- App groups and app catalogs can be created to push specific sets of apps to the devices of students and teachers of different grades.
- Can update the apps automatically or on-demand.
- Can monitor the app status from the EMM portal.
- Setting the apps as mandatory helps in identifying the devices on which the apps are not installed. This feature is extremely useful in preventing students from removing any essential apps from their devices.



"It was a breeze to install the app. I really had no major issues that I could point to and say that's Hexnode's issue."

Joshua McHugh

IT Admin at SKS

Remote management

- Hexnode Messenger, the messaging module from Hexnode, helps in broadcasting important messages to the student devices at remote locations. The messenger also comes in handy in device troubleshooting.
- Remote actions like the remote lock, device scan, location scan, clear passcode etc., help manage devices without being manually present and physically accessing them, which saves a lot of working hours.
- Battery levels and activeness of the devices can be remotely monitored from the EMM portal.
- OS updates can be pushed or delayed for a remote device.
- For devices supporting remote monitoring and control via EMM, device troubleshooting, student evaluation etc., are quite easy.

"It just makes life so much easier. Okay, if we need to reset an Android tablet what we will have to do is to link it to Hexnode...
...all the apps for each department just get automatically installed."

Ryan Boundy

ITC at Sir John Hunt CSC

Security management

- Restrictive control over the device, like disabling the SAFE mode access, helps in preventing the students from manipulating or making unwanted alterations to the device settings.
- Web content filtering ensures online security by preventing access to non-educational websites.
- Password policy provides a basic layer of security for the device and makes sure that the device is used only by the intended user.
- Tracking the device's geographical location helps pinpoint lost, misplaced or stolen devices. The current location and location history of the devices can be easily obtained from the EMM portal.
- The option to block the installation of malicious applications is an added security feature on the devices.

"We used Hexnode to manage and secure mobile devices deployed to junior school students."

Clive Henley

IT Manager at Heritage Christian School

Containerization

- Personal devices of teachers and students used for teaching and learning purposes respectively can be enrolled with the Android Enterprise program or enforced with the Apple Business Container restrictions to separate personal and work data.
- Android Enterprise Profile Owner mode helps separate sensitive data from personal data and manage it separately, giving users better privacy.
- Android Enterprise Device Owner mode gives full authority for the enterprise IT over company owned devices.

"Hexnode makes it a lot easier to get all our work done on a day-to-day basis... It really helps to reduce our workload"

David Powers

District Police/ Patrol officer at Austin Community College

Device lockdown

- Turning out a device into a kiosk helps ensure that the students can access only the essential apps and features and nothing else from the device.
- The Hexnode Messenger can be used to share instructions even when the student devices are in the kiosk mode.
- The restricted and purpose-specific mode ensures that the students couldn't tamper with the device settings and use the school owned devices for their personal needs. School owned Android devices, for instance, can be enrolled Android Enterprise Device Owner and locked down to the kiosk mode.
- Website kiosks can also be set up with only education websites and admission websites in which the student details are to be filled up on the device.

"The product has performed as advertised. I think that the most important area that I have to deal with is the support. The tech help has been stellar. I have never had a negative experience with Hexnode. A++ rating"

Larry Franks

IT Admin at Hartley ISD