Connected Learning Advisory
Te Ara Whītiki

Device deployment, customisation and ongoing management

Photo by Hal Gatewood on Unsplash

The way in which digital devices are set up (deployed), customised and managed is crucial to ensure they provide the experience that students and staff need in a cost-effective, secure and efficient way. This guide outlines how schools and kura should be planning to deploy, customise and manage the devices they own or lease as well as the devices that staff or students might want to bring and use.

Summary of recommendations

- Use cloud-based mobile device management (MDM) systems to support the types of devices you have.
- Seek technical support with setting up your MDM systems.
- Consider carefully whether or not you enable any management of BYOD devices.

Contents

Once you have read this guide you are welcome to contact the Connected Learning Advisory to get more personal assistance. We aim to provide consistent, unbiased advice and are free of charge to all state and state-integrated New Zealand schools and kura. Our advisors can help with all aspects outlined in this guide as well as provide peer review of the decisions you reach before you take your next steps.

For more information visit www.connectedlearning.org.nz
Check out our resources at resources.connectedlearning.org.nz
Call us for personalised service on 0800 700 400
Make a personal inquiry via our online form at query.connectedlearning.org.nz
Email info@connectedlearning.org.nz

Definitions

For the purpose of this guide:

Device - any kind of computer, laptop, tablet, smartphone or hybrid.

Deployment - moving a device from its current state to a desired state that is ready to be customised. Deployment usually involves resetting or reloading the operating system so it is clean of any previous customisations.

Customisation - making a device ready to be used such as by configuring wifi or printer settings, installing apps/software, naming the device, setting desktop or screensaver images, enforcing technical policies, etc.

Management - the ongoing intervention needed to maintain a device such as tracking it, providing or checking security updates or adding and removing apps/software.

How the deployment, customisation and management landscape has changed

Until relatively recently, the majority of digital devices in schools were desktop computers which tended to be deployed, customised and managed on a cabled network using a server. However, this has changed significantly through a number of developments:

- Fast, ubiquitous wifi and Internet connectivity has enabled devices to be mobile and wifi-only. This means the devices themselves can be anywhere and they can be managed from anywhere: there is no reason to be restricted to a particular physical location.
- A move towards ongoing, more regular updates to software and operating systems every few months rather than on a 3-5 year refresh cycle.
- A greater variety of device types and operating systems that schools want to deploy and manage: Microsoft Windows, Apple Macs, iPads, Chromebooks, Android tablets, Linux and others.
- The expectation that people should be able to have a more configurable and personal user-experience on any device and at any location, rather than a generic or technically-determined one.
- The desire for devices to be available for use at all times rather than having to be out of action while being reconfigured.
- People wanting to get the benefit of new functionality, apps or updates as soon as they are available instead of having to wait for months or even years for them to be made available through technical support.
- Schools seeking greater cost-effectiveness by moving away from having to procure and manage on-premise

servers towards using cloud-based services on monthly subscriptions or no-cost basis.

These days, devices have tended to become more personal such that deployment, customisation and management can be done by the owner of the device via a series of set-up prompts and customisations such as:

- Entering Wifi network settings
- Entering language or region settings
- Accepting terms and conditions
- Registering or licensing the device or its apps / software
- Installing and configuring apps / software / updates / scripts / settings
- Configuring the device so that the user experience is specific to their needs
- Managing the device by installing updates, clearing off old files, etc.

For a large number of devices, whilst it might be possible to undertake these kinds of steps manually one-by-one for each device, it is not generally recommended to do so because it:

- is time-consuming
- carries the risk of human errors
- can end up with inconsistencies

Sometimes, though, such a hands-on, manual approach to deployment, customisation and ongoing management can make sense, especially if:

- There are only a few devices to deploy
- The amount of re-configuration is minimal
- The device is not shared

Automation using a Mobile Device Management (MDM) System

Automation used to only be possible using a local server but now there are many cloud-based Mobile Device Management (MDM) systems that can be used. We recommend that schools consider one or more MDM systems to help with the deployment, customisation and ongoing management of their devices. Microsoft, Google and Apple all support and recommend such a cloud-based MDM approach for their operating systems as outlined in the appendix.

Ordinarily, automating the deployment, customisation and ongoing management of devices will provide a more consistent, secure and cost-effective outcome when there are more than approximately ten devices involved.

Features and benefits of MDM systems

Mobile device management systems typically offer the following features and benefits. Each MDM will vary, though, in the features they have available and how they work so it will be essential to check them out carefully before making a decision about what to use.

Typical features

- An inventory / asset register of attributes such as devices' serial numbers, names and location
- A view of the apps/software, settings and security updates that are running on devices
- The ability to remotely configure apps/software, scripts and settings in an automated way
- Scalability from a few devices to a few thousand

Common benefits

- Users and groups can have their experience customised based on their specific needs
- Customisations like new apps/software, updates, scripts and settings can be made readily and on the fly in an agile, automated way whenever changes are needed
- Analysis of device usage can inform decisions around future device purchases and deployments
- The location of devices can be determined if devices go missing
- Administrators can check that the right apps/software, updates, scripts and settings have been properly installed on devices to ensure their usability and security
- The hands-off approach made possible by MDM's should save time and means changes can be done more easily and cheaply
- People's experience when using devices should be reliable and consistent which will increase their readiness to use the them

Can one MDM system manage all types of devices?

Microsoft and Apple have both opened their operating systems to being managed by third party MDMs whereas Google’s devices can only be managed by the Google Admin Console using the Chrome Education License.

Using the same MDM system to manage both your Apple and Microsoft devices should be considered as this will reduce the number of tools that need to be learnt, accessed and paid for.

What costs are involved to use an MDM system?

Subscription costs
MDMs are typically purchased on a monthly subscription basis, although some are at no cost, including options available in the Ministry’s Microsoft Schools Agreement. The cost of the MDM should be considered alongside the alternative (if it exists) of purchasing and running a server and software to manage the devices at your school. Simplifying the management of devices with MDMs should lead to cost-savings through reduced technical support time.

Technical support costs
Configuring and managing an MDM is technically involved. You should work with a technical support company to give you assistance with the initial configuration. Once set-up, using the MDM should be easy enough with some training and familiarisation.

Using the capabilities of the MDM to proactively manage devices requires somebody to be responsible for the monitoring of the information that the MDM provides; installing an MDM then having nobody responsible to monitor it would be a waste of time and money! The monitoring could be done by a school support staff member or a technical support provider.

Which devices should you manage using a MDM system?

School-owned devices

School-owned devices should be enrolled in an MDM given the benefits outlined above.

TELA devices

There are also advantages to using an MDM for TELA devices - in particular the ability to confirm whether the devices are running the latest security updates.

TELA+ can support schools in using Apple's Device Enrolment Programme and Microsoft's AutoPilot which allow a device to be automatically enrolled in the school's MDM before it ships to the school. Google's Chrome Education License must be purchased separately.

Student or teacher owned devices

Careful consideration is needed to determine whether students' devices should be enrolled and managed by an MDM. Some factors to explore include:

> **Cost:benefit ratio**: is the financial outlay of the MDM worth the benefits of having student devices managed?
>
> **Demarcation**: by enrolling a device in a MDM the school has some controls over that device. The school may not want to have this increased responsibility.

Making the MDM optional for students and pointing out the advantages of using it may be a suitable approach.

Can we change from one MDM to another?

As MDMs are managing settings that have been enabled on the operating system they tend to be differentiated on price and their user interface rather than on what settings they are capable of configuring. This means there is little risk of a school being locked in to a particular MDM solution with a proprietary configuration.

You should expect a similar amount of work to move from one MDM to another as was involved in setting up your original MDM.

Considerations for choosing a MDM system

Talk to the Connected Learning Advisory, other schools and your technical support provider to ask for recommendations.

There are many MDM options on the market. Our recommendation is to consider a product that is proven to work well in schools in New Zealand and that offers features and support most relevant for you at the right price. You should note:

- All MDM solutions will have an associated labour cost to deploy and manage.
- Learning to use a new MDM is complex and time-consuming.
- Using MDM systems will be essential for schools with many devices.
- As a long term strategy, aim to use an MDM with known costs that will support your future needs.
- A robust wireless network is essential for MDMs to work well.
- It is important to be clear about what a particular MDM can deliver and how easy it is to use.
- Look for an MDM that is regularly updated to support the latest features.
- You are likely to need to work with a technical support provider that has proven experience with one or more MDMs.
- Consider the cost- and time- saving benefits of using an MDM that can support multiple operating systems

Further Support and Useful Links

Connected Learning Advisory guides:

Deploying School iPads

Planning and Managing a Chromebook Deployment

Vendors' guidance for device deployment in schools:

Microsoft devices

Apple devices

Google devices

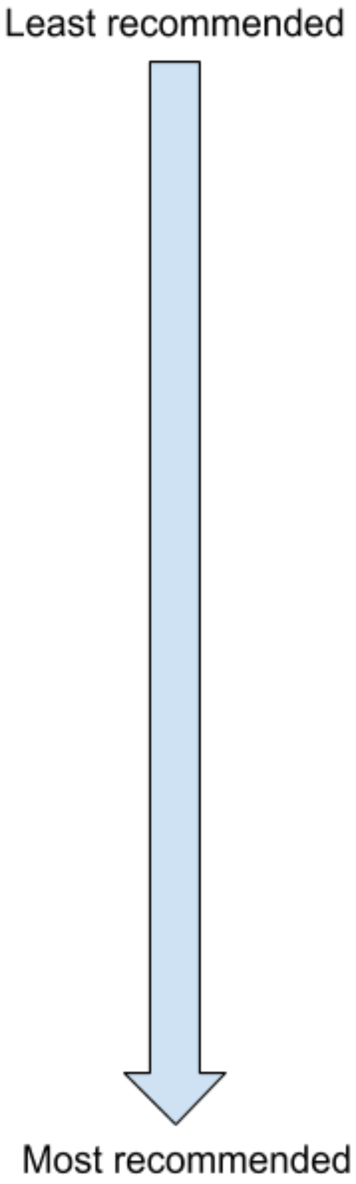
This guide has been produced in response to a number of specific queries about device deployment, customisation and ongoing management from schools. It should not be read as a recommendation or endorsement of any specific product. The Connected Learning Advisory is a Ministry of Education supported service that provides schools with technology information relevant to their queries and does not recommend one product over another.

Date Last Updated:	28th August 2018

Appendix: Suggested Deployment, Customisation and Management Approaches for Different Devices

The following outlines the suggested approaches for the most common types of devices in New Zealand schools.

Device Deployment Options
The four common ways in which devices are deployed are outlined below in order from least recommend to most recommended:



Imaging

In the past, a common way to deploy devices was to set up a master device with the settings and configuration that was required then to capture this as an ‘image’ which is used to deploy to other similar devices. This method worked well with consistent hardware on a fast, wired network but nowadays does not provide the agility that is demanded with a school typically having a wide variety of devices. Also, for many types of operating system the imaging approach is not technically possible.

OS Deployment

Pushing a new operating system to a device is possible in some cases but typically requires a high level of technical expertise to achieve. It is also likely that pushing an operating system over wifi is slow and troublesome so using USB sticks or a wired network (if devices have an ethernet port) may be necessary.

Resetting

Many types of device can be used out of the box or reset back to their original operating system. Then, using a Mobile Device Manager or other system to automate the deployment process means the devices can be provisioned with minimal hands-on time.

Device Enrolment

Some operating systems allow for the device’s serial number to be registered with the manufacturer as belonging to a particular school. Once the device is connected to the internet, a Mobile Device Management system recognises it and applies the school’s apps / software / updates / scripts / settings accordingly. This approach is the most hands-off of all, with the end-user being able to use the device straight from the box once it has been connected to the Internet.

Microsoft Windows Devices - Desktops, Laptops, Tablets, Hybrids

Overview

Devices running Microsoft Windows have traditionally been deployed and managed by a server at school. However, once they are running Windows 10 Pro, Education or Enterprise, Windows devices can now be managed by a MDM, albeit with a more limited toolset than the on-premise server solution can provide. Using a MDM to manage Windows 10 devices is much simpler than setting up and maintaining Windows servers.

The cloud-based Microsoft Azure platform holds the school's user accounts and information about the Windows devices enrolled. Users should have accounts in Azure Active Directory (AAD) so they can have their settings and files synced when they log in to different devices. Joining devices to the Azure AD will enable your users to log in to your Windows devices using their school user accounts.

Schools should all now be deploying Windows 10 to devices and running the Education, Pro, or Enterprise edition on them so that they can be joined to the Azure AD and get the benefit of the full MDM feature set that Microsoft enables MDM systems to access. However, it is also possible for a Windows device to be managed by a MDM just by being registered with the Azure AD. This means BYOD devices and those running Windows 10 Home edition can also be provided with some more limited management capabilities.

Deployment Options

Imaging - This is possible but not recommended as maintaining and updating the image is too hard.

OS deployment - Devices that ship with Windows 10 Home edition will need to be upgraded to Windows 10 Education, Professional or Enterprise edition by reinstalling the operating system. Similarly, devices running previous versions of Windows should also have a new operating system installed. This can be done by using a local USB drive or across the network using a Network Attached Storage (NAS) device if wired ethernet ports are available. Technical support is likely to be required to do this.

Resetting - Windows 10 devices can be easily reset with a fresh installation of Windows 10 from the *Settings* menu.

Device Enrolment - Windows Autopilot can be used to ensure a device gets automatically set-up for a particular user out of the box.

Management Options

Microsoft enables any MDM provider to manage its Windows operating system. It also has its own MDM, Intune. There are two versions of Intune as outlined in this blog post - When To Use Intune For Education vs Full Intune Standalone. The Intune for Education product is provided by Microsoft at no cost to all schools globally. Full Intune Standalone is provided at no cost to NZ state and state integrated schools as part of the Microsoft Schools Agreement. Intune is likely to provide a superior feature-set and compatibility than a third-party MDM.

Apple MacOS Devices - iMacs, Macbooks

Overview

In the past MacOS devices have typically been either unboxed and left unmanaged or re-imaged using utilities such as DeployStudio, Casper and Munki and managed using Apple Server, third-party tools like JAMF Casper or Windows Active Directory.

Deployment Options

Imaging - For the current Mac operating system, Macs can have their OS installed but cannot be imaged to include a full software set and configuration.

OS Deployment - This can be done by using a local USB drive or across the network using a Network Attached Storage (NAS) device. Technical support is likely to be required to do this.

Resetting - Macs can easily be reset using the ‘restore’ process.

Device Enrolment - Macs can be automatically enrolled in an MDM using the Device Enrollment Programme (DEP).

Management Options

Apple enables any MDM provider to manage devices running its MacOS operating system. It also has its own MDM, Profile Manager, but this is not recommended to be used for anything other than testing purposes. There are many third party MDM options to manage Macs.

Apple IOS Devices - iPads, iPhones

Overview

iPads were initially difficult to manage as multi-user devices as they were designed as a single-user device. However, Apple now has well-developed solutions for them to be deployed and managed effectively.

Deployment Options

Imaging - IOS devices cannot be imaged

OS Deployment - In extreme cases it is possible to re-deploy the IOS using iTunes but this is uncommon.

Resetting - IOS devices can easily be reset from the *Settings* menu.

Device Enrolment - iPads can be automatically enrolled in an MDM using the Device Enrollment Programme (DEP).

Management Options

Apple enables any MDM provider to manage devices running its IOS operating system. It also has its own MDM, Profile Manager, but this is not recommended to be used for anything other than testing purposes. There are many third party MDM options to manage iPads.

We recommend using DEP and an MDM to manage Apple IOS devices.

Google Chrome OS Devices - Chromebooks, Chromeboxes

Overview

The Google Admin Console is the centralised point of management for Chrome devices. This requires a Chrome Education License to be purchased and allocated to each Chromebook. Without the license, Chromebooks can still be logged in by users as long as they have a personal or school-managed Google account.

Deployment Options

Imaging - Chrome devices cannot be imaged.

OS Deployment - In extreme cases it is possible to re-deploy the Chrome OS through ‘Powerwashing’ but this is uncommon.

Resetting - Chrome devices can easily be reset and this is the most common way to re-deploy them.

Device Enrolment - Chrome devices can be enrolled automatically into the Google Admin Console if a Chrome Education License is purchased.

Management Options

Google only enables third-party MDMs to access basic information about Chrome devices. It is only possible to apply a configuration to a Chrome device through the Google Admin Console.

By purchasing the Chrome Education Licence, the ability to control, administer and set policies greatly reduces the amount of effort to manage Chrome devices. A one-off license may be purchased for each Chromebook that you wish to manage. The license is specific to the model of Chromebook purchased, but not to the actual device itself. While Chromebooks are very usable without purchasing the Chome Education License, we recommend that the reduction in time and effort required to manage the devices, along with the features and benefits that the license enables, makes the additional cost of the license worthwhile.