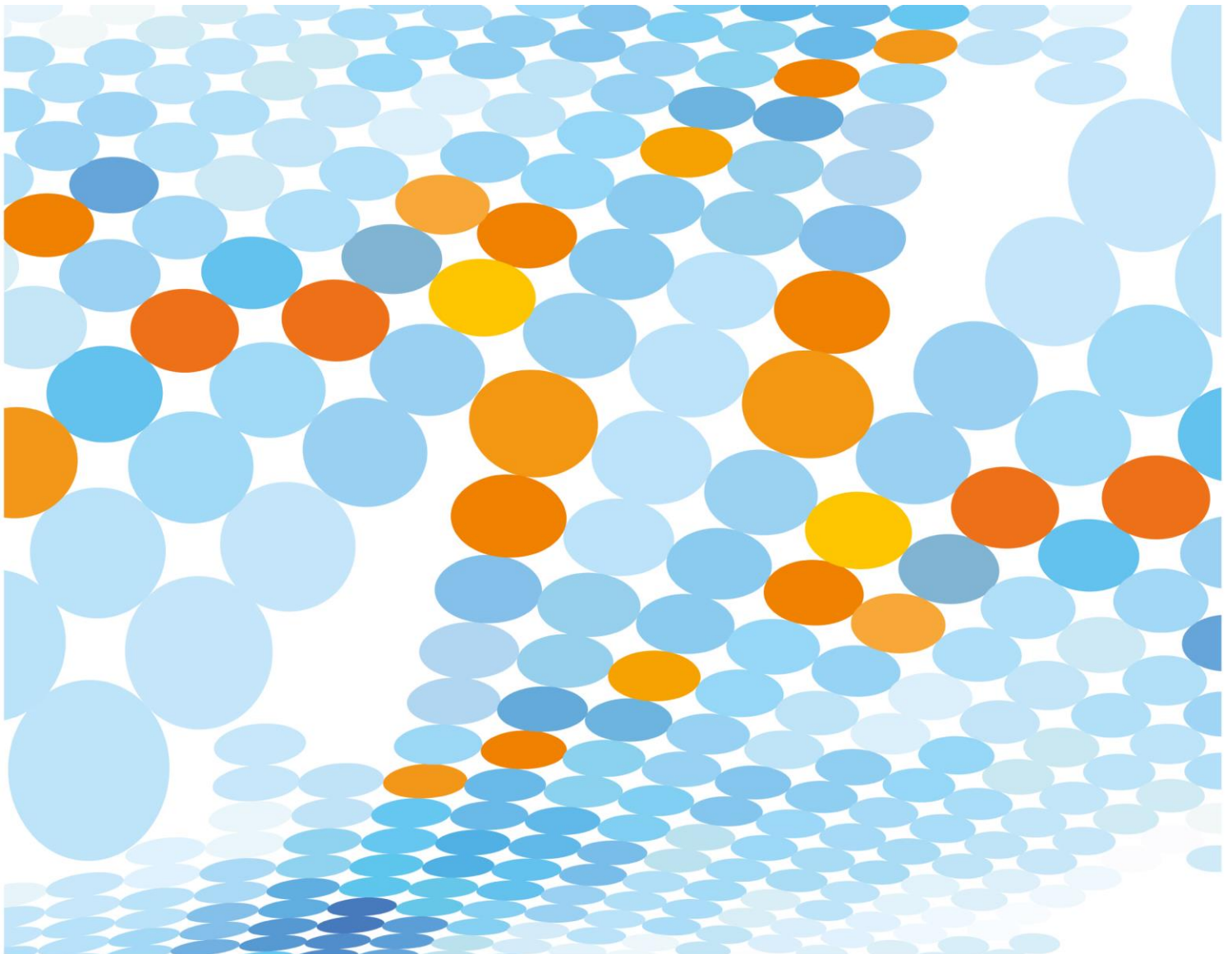Fact Sheet - Pilot

Using MS Intune, for Queensland State Schools

A significant number of Queensland State Schools are engaging in Bring Your Own Device (BYOD) programs. To enable students to easily access departmental resources on their own devices, the Department of Education is implementing 'Enterprise Mobility Services': a suite of products including 'Microsoft Intune'.

What Intune does

This software enables mobile configuration settings to be deployed to devices to:

- Enable Wi-Fi Connectivity to the school's network

- Enable automatic setup of the device's default mail application to add the student's departmental email account

- Enable access to a school selected list of mobile or store applications

- Enable access to a school selected list of websites

- Enable students and central office support staff the ability to remove the device from Intune

- Enable students the ability to 'factory reset' a lost or stolen device. Students can perform this remotely via the self-service console http://portal.manage.microsoft.com.[1]

- Provide information on applications installed through Intune[2]

- Provide some information such as username, device serial number, device name, model, manufacturer, OS name and version

What Intune does not do

- Monitor student's use of the device

- Track student's locations

- Provide information on personally installed applications[3]

- Allows uninstalling of personal applications

---

1 While central office support staff also have the ability to 'factory reset' a device, they will never perform this function due to the destructive nature of the process.
2 Some devices differ in the information gathered or the amount of control provided by that device type. For example, IPads support a complete factory reset if desired, however Android devices do not.
3 Due to the way Apple has configured MDM capability for MacOS, Intune reports ALL software applications installed on Macs

How does a student enrol a device?

Microsoft has provided detailed guides regarding the enrolling procedure for all devices. Please see the attached PDF document for quick instructions.

Please note that you can click on any of the icons below to access YouTube instructional videos.

Alternatively, Microsoft documents can be found via the links below.

Device Type	Document URL
iOS (IPhone & IPad)	https://docs.microsoft.com/en-us/Intune/EndUser/enroll-your-device-in-intune-ios
Windows 10	https://docs.microsoft.com/en-us/intune/enduser/enroll-your-w10-phone-or-w10-pc-windows
Android[a]	https://docs.microsoft.com/en-us/intune/enduser/enroll-your-device-in-intune-android
Mac OSX	https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-macos-cp

---

[a] Although Android devices work well through Intune at home due to the way the school internet works Android applications may not work at school.

How does a student install school applications?

In the Company Portal application or website http://portal.manage.microsoft.com, click on *View*, then choose from the school-selected list of applications available to install. These applications link directly to the device's registered app store, so when an application is updated on the store, the update will be available for that app on the device.
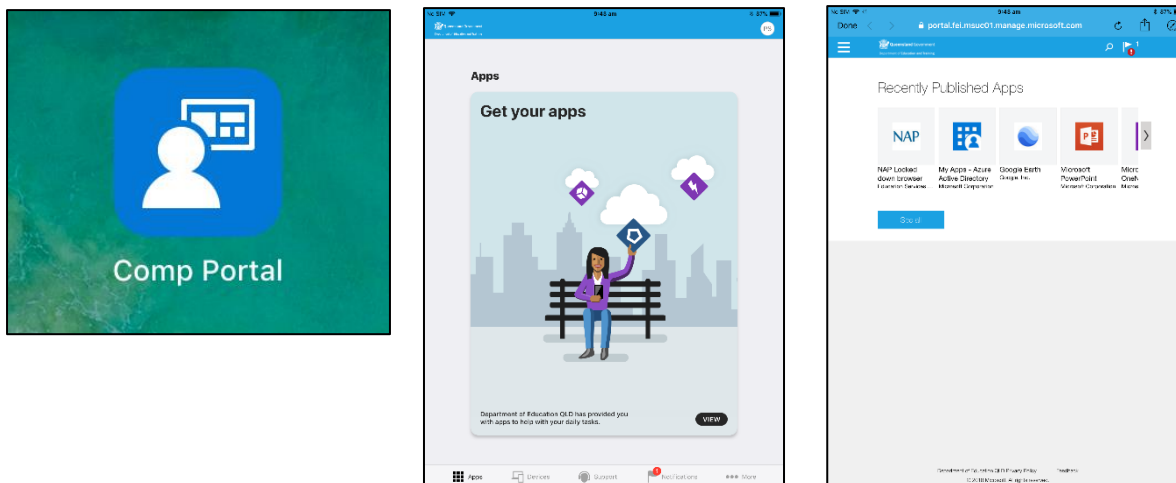
How does a student access the list of school-selected websites?

EMS comes with access to a web portal called *Azure Access Panel* or *My Apps*. The website https://myapps.microsoft.com/, or application acts as a single sign-on portal to any websites for which the department and school has configured access. The department undertakes a rigorous approval process for storage of any student information captured in non-departmental managed systems. The applications identified in this Launchpad support two types of logging on. One utilises the student's departmental identity, which can include information such as username, first name and last name. The other logon process allows a student to save their own unique username and password for a particular application within the portal itself. This method pre-populates the username and password when the student clicks on that website link, so that minimal user intervention is required.
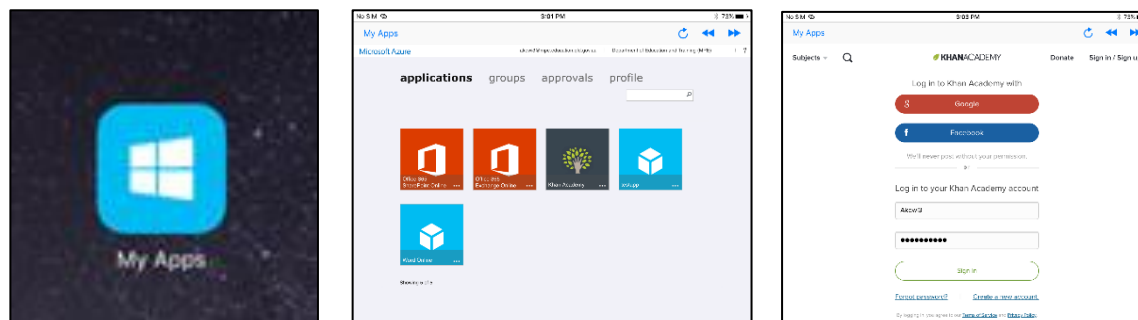
Frequently Asked Questions

Why do I need to enrol my child's device in Intune if it has already been setup for connecting to the school network?

Although connecting to the school network may have already been established on your child's device we would encourage you to enrol the device into Intune. As technology including Wi-Fi is consistently changing, installing Intune will allow us to automatically update your device with the correct settings.

Some of the other benefits of enrolment are:

- Access to a list of school endorsed applications and websites applicable for your device.
- Automatic setup of school email
- The ability for your child to self-manage their device

Will my child's device utilise my home internet data allowance when enrolled in Intune?

A small amount of data is required when the device is online and connected to either Wi-Fi or a mobile service. This is minimal, however, as no applications other than the *Company Portal* app on Windows devices and configuration profiles are automatically pushed to the device. For this reason, we recommend devices be connected to the home Wi-Fi for the initial enrolment process to avoid any potential mobile service charges.

Will the Department of Education or school ever deploy applications to my child's device?

With the exception of the *Company Portal* application during the enrolment process on Windows, departmental support staff will not automatically deploy applications to devices. This is to ensure unexpected data usage is not encountered and will enable the student to select which applications are relevant to their learning from the school-selected list.

How do I un-enrol my child's device?

Currently there are two ways to un-enrol a device:

Option 1 On the device - open the *Company Portal* application. Under *My Devices* click on the device you wish to remove and then click *Remove*.

Option 2 If you do not have physical access to the device, logon to http://portal.manage.microsoft.com via any web browser. Under *My Devices* click the device you wish to remove and then click *Remove*.

Can I continue to use my device as a personal device once enrolled?

Yes, you can. No settings or applications installed via Intune will impact the ability to use the device as normal. It is worth noting, however, that the configuration of connecting the default mail application to your child's departmental email account does enforce enabling a pin code or a password for Windows to unlock the device. This is good practice for your child to learn and has been implemented with cyber safety and security in mind.

Can my child enrol more than one device?

Yes. Each child can enrol up to five devices.

Can my child's device be enrolled in more than one Mobile Device Management (MDM)?

No. A device may only be enrolled in one MDM.

Controls may be enforced at home as follows

- For iOS and Mac OS devices use **Parental Controls**

- For Windows devices use **Microsoft Family**

Both facilities are compatible with Intune.

Is there any cost associated with using Intune?

The department does not impose a charge for the use of Intune. Your child's school may impose charges for supporting BYOx or application licensing costs, however, this is separate to Intune.

What devices are supported with current DoE implementation of Intune?

Currently Intune supports Android 5.0+[4], IOS 10.0+ (IPad & IPhone), Mac OSX 10.11[5], Windows 10 (not Windows 10s), and Windows Phone.

Who do I contact if I have trouble using the EMS or Intune?

Please contact the school administration office if you have any issues enrolling your device or have any concerns with the management of this product.

---

[4] Although android is supported, connecting to the school internet is not supported so connectivity has to be achieved at home or through a non-school network.
[5] Mac OSX support is limited to Wi-Fi and email profiles. Application installation is not supported at this time.

My child's Android device says their activity may be monitored or their iOS device says when enrolling that the administrator may collect personal data and other undesirable activities. What does this mean?

These warnings are specific to the Operating System of the device. By enrolling the device into a Mobile Device Management platform, like Intune, there are some inherent permissions the platform can use. Intune only utilises some of the capabilities, which have been detailed in the table below.

Attribute	iOS	Windows	Android	MacOS
Device Name	Y	Y	N	Y
Operating System Version	Y	Y	Y	Y
User Enrolled	Y	Y	Y	Y
Model	Y	Y	Y	Y
Serial Number	Y	Y	Y	Y
Last 4 digits of phone number	Y	N	N	N
Last Check in Time	Y	Y	Y	Y
Storage space	Y	Y	N	Y
IMEI Number	Y	Y	Y	N
Carrier	Y	Y	Y	N
MAC Address	Y	Y	Y	Y
Personal Apps	N	N	N	Y
Intune Apps	Y	Y	Y	Y