Solution

Intune is being used to enable connectivity to school Wi-Fi and provide access to school applications, although Intune and other MDM's have management capability and stricter controls can be enforced this is not enacted for personal devices. Intune as a product also limits visibility and actions that can be taken on personal devices.

What can school administration staff see or not see on a personal device?

What Intune administrators can see on personal devices	What Intune administrators cannot see on personal devices
Your school can only see information that may be relevant to the school:	Your school does not monitor use of the device:
Device owner.	Cannot see your child's personal information.
Device name.	Cannot see what your child is doing on their device.
Device model.	Does not track student's locations / device location.
Device manufacturer.	Does not provide information on personally installed applications.
Operating system and version eg: iOS 13 or Windows 10.	Does not allow uninstalling of any applications including your child's own applications.
Apps managed by Intune only not personal apps	Home Network cannot be seen.
Device serial number and IMEI.	Cannot see calling and web browsing history.
Storage space	Cannot see Email and text messages.
	Cannot see contacts.
	Cannot see calendars.
	Cannot see passwords.
	Cannot see pictures, including what's in the photos app or camera roll.
	Cannot see files.

What actions can be taken by who on personal devices?

End users who enroll their own devices can remotely unenroll and wipe their own devices.

School based staff, Regional support staff and Service Centre staff only have the permissions delegated to be able to assign applications to users, no other actions can be undertaken.

A small subset of Central office third level Intune and Office 365 support staff have the permissions delegated to take further actions but have been advised through an Intune standards of practice what actions can be taken on personal devices.

What is the Intune Administrators standards of practice?

This document contains a table of capabilities, controls and recommendations to ensure that personal device autonomy is maintained by users and Intune administrators do not adversely affect users and devices.

Below is the contents of the document:

<table>
<tr><th>Capability/Function</th><th>Considerations</th><th>Capability Available</th><th>Determined Best Practice</th></tr>
<tr><td>Assigning Applications to Personally Owned Devices</td><td>Mandatorily deploying applications to devices may incur data usage costs depending on client networks.</td><td>Intune does allow applications to be "required" on devices. This control is delegated to the School Admin, Service Centre, Regional System Technicians and Intune Global Admin. The technology does not allow limiting this control to only "offer" applications.</td><td>Only assign an application as required to Device Groups which contain school devices, these are currently <Schoolcode>_iOS_Staff, <Schoolcode>_iOS_Shared, <Schoolcode>_iOS_Student, <Schoolcode>_iOS_Kiosk and <Schoolcode>_MacOS_Shared.

Do not assign an application as “required” to user groups, instead always select “available” this will empower the user to select when to download and install the application.</td></tr>
<tr><td>Remotely factory resetting a device</td><td>Performing a factory reset on a device is likely to remove all user data, settings and restore the device to ‘as new’ software condition. This is a major destructive operation on a device especially a personally owned device.</td><td>Although capability exists in Intune to factory reset a device, School, RST and Service Centre Delegated control does not allow this to be performed except on School owned devices. Only Intune and Office 365 Global Administrators have the capability to do this to personal devices.

Also note Android devices do not support factory reset.</td><td>End users can remotely perform this task for their own devices from the Intune user portal https://portal.manage.microsoft.com this method is only recommended for a lost or stolen personal device.
No administrators will perform this task on personal devices due to the risk of personal data loss.
School owned devices can be reset by <schoolcode>_MISAdmins and Service Centre, Regional System Technicians and Intune Global Admin can provided evidence of school consent has been provided.</td></tr>
<tr><td>Un-enrolling a device</td><td>Un-enrolling from Intune can remove all Intune provisioned Applications, Certificates, Profiles and settings. This action does not remove user applications, personal files or other settings.</td><td>All operating systems are supported in Intune for remote un-enrolment.
Only Intune Global Administrators would have this capability.
End users can perform this task from either the company portal app or remotely from the Intune user portal https://portal.manage.microsoft.com.</td><td>It is recommended that only end users perform this action. Due to the potential for teaching and learning disruption.</td></tr>
<tr><td>Deleting a device from Intune.</td><td>If a device gets re-imaged or retired without un-enrolling or wiping from Intune, the device can remain in Intune for up to 270 days. Personal devices can be un-enrolled and then deleted through the Intune Admin Portal.</td><td>Only Intune Global Administrators would have this capability.</td><td>Stale or orphaned devices will cycle out automatically after the 270 day cycle. Users should be encouraged to un-enrol if they are leaving the school permanently.</td></tr>
<tr><td>Intune inventory information on personally owned devices</td><td><table>
<tr><th>Attribute</th><th>iOS</th><th>Windows</th><th>Android</th><th>MacOS</th></tr>
<tr><td>Device Name</td><td>Y</td><td>Y</td><td>N</td><td>Y</td></tr>
<tr><td>Operating System Version</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>User Enrolled</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Model</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Serial Number</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Last 4 digits of phone number</td><td>Y</td><td>N</td><td>N</td><td>N/A</td></tr>
<tr><td>Last Check in Time</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Storage space</td><td>Y</td><td>Y</td><td>N</td><td>Y</td></tr>
<tr><td>IMEI Number</td><td>Y</td><td>Y</td><td>Y</td><td>N/A</td></tr>
<tr><td>Carrier</td><td>Y</td><td>Y</td><td>Y</td><td>N/A</td></tr>
<tr><td>MAC Address</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td>Personal Apps</td><td>N</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td>Intune Apps</td><td>Y</td><td>Y</td><td>Y</td><td>Y</td></tr>
</table></td><td>All Intune state wide delegated admins (Service Centre, Regional System Technicians and Intune Global Admins) can see ALL devices enrolled. School admins can only see personal devices for schools which they are MIS Admins of.</td><td>Similar to on-premises Active Directory, devices are listed with their attributes in a global list. There is limited amount of visibility control that can be enforced. End users will need to be conscious of accepting enrolment conditions which are enforced through their own operating system platforms. The MIS terms and conditions must also be agreed to before enrolment will proceed.</td></tr>
</table>