MDM – Mobile Device Management of Staff-Owned Devices

Lincoln College Staff Guide
Version 1.0

Author: IT Services
Date: 14.09.2022

Contents

Why?

Lincoln College is required as a condition of ESFA funding and cyber insurance to achieve the cyber essentials accreditation. This also helps maintain a good level of cyber security.

Each year the accreditation changes in order to maintain relevance and to keep pace with technology and security threats.

This year all computing hardware that accesses any college systems or data is in-scope including personal devices such as mobile phones, tablets and laptops and must meet a set of requirements before being classed as compliant.

To meet these new requirements staff who wish to access any IT resource[1] provided by the college using personal equipment must self-enroll into the Microsoft In-Tune system. This records information about your device enabling the IT department to verify the device health and security before granting access.

Please see Appendix I and II for further details about the Microsoft InTune system.

[1] Microsoft Office 365 (Outlook, Word, Excel, Onedrive, Teams) either via MS Office or a web browser Remote Desktop Gateway

Requirements for Staff-Owned Devices

Personal Computers, Laptops and Macs

Personal computers must be under manufacturers support (not to be confused with manufacturer warranty)

Supported Operating System with latest updates and patches installed

Recommended: Windows 10 or 11

Minimum: Windows 10

Recommended: MacOS 11 or 12

Minimum: MacOS 10.15

Firewall enabled

Anti-Virus enabled and up to date

Mobile Devices, Smart Phones and Tablets

Mobile devices must be under manufacturers support (not to be confused with manufacturers warranty)

Supported Operating System with latest updates and patches installed

Android Recommended: Version 11,12 or 13

Android Minimum: Version 10

iOS Minimum: Version 13

iOS Minimum: Version 14,15 or 16

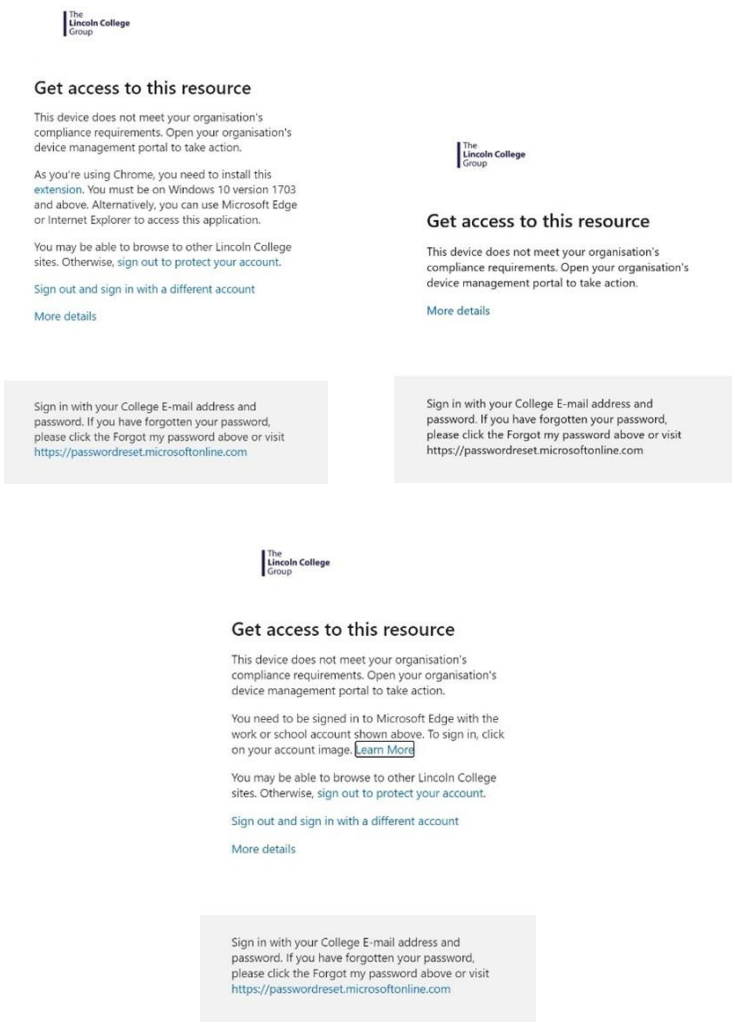
Pin or Biometric screen lock

Not jailbroken or with an unlocked bootloader[2]

[2] This is where a mobile phone has been unlocked in order to install operating systems (iOS and Android) or other software that was not intended to be used on that device by the manufacturer.

Blocked Access – What will Happen to Devices that do not have InTune

When you try to access Lincoln College IT resources using a home device that does not have InTune installed you will receive a blocking message like one of these -



If you see a blocking message please proceed to the next stage …

Device Enrollment

Personal Computers, Laptops and Macs

Please refer to the separate guide on enrolling personal computers.

Personal Computers, Laptops and Macs

Please refer to the separate guide on enrolling Mac computers.

Android Phones

Please refer to the separate guide on enrolling Android devices.

Apple iPhones

Please refer to the separate guide on enrolling Apple iPhone devices.

Appendix I – What can the IT department see and do using Microsoft InTune?

Taken from https://docs.microsoft.com/en-us/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

Things your organization can never see

- Calling and web browsing history
- Email and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what's in the photos app or camera roll
- Files
- Additionally, on corporate-owned Android devices with a work profile:
- Apps and data in your personal profile
- Phone number

Things your organization can always see

- Device owner
- Device name
- Device serial number
- Device model, such as Google Pixel
- Device manufacturer, such as Microsoft
- Operating system and version, such as iOS 12.0.1
- Device IMEI
- App inventory and app names, such as Microsoft Word
- On personal devices, your organization can only see your managed app inventory, which includes work and school apps.
- On corporate-owned devices, your organization can see all apps installed on the device.
- On corporate-owned devices with a work profile, which is limited to Android devices, your organization can only see the apps installed in your work profile.

Please note that should a staff-owned device be stolen, or compromised by cyber attackers, the IT department reserve the right to wipe the device to avoid college data being used by hackers or criminals to ransom or extort the college.

Appendix II - What happens after I enroll in Microsoft InTune?

Taken from https://docs.microsoft.com/en-us/mem/intune/user-help/what-happens-if-you-install-the-company-portal-app-and-enroll-your-device-in-intune-windows?source=recommendations

When you enroll your Windows device (mobile or desktop), you are giving IT support permission to:

- You can access your org's network, email, and work files.
- You can install work or school apps from the Company Portal website and app. (Note: for Windows 7 and Windows Vista, you can only get these apps from the Company Portal website.)
- Your work or school email is automatically set up.
- You can reset your phone to factory settings if it's lost or stolen.
- What happens on Windows PCs after enrollment
- In addition to everything under What happens on all devices after enrollment, after you enroll a Windows PC in Intune:
- Software is installed on the computer so that IT support can manage the computer. IT support can automatically update this software.
- Intune Endpoint Protection might be installed on your computer. This software checks for viruses and malware.
- IT support can't view or make changes to anything on your hard drive but Intune needs access to the hard drive on your Windows device to make sure that it's configured to meet your organization's device/security requirements. This is the same kind of access that Intune needs on a mobile device (for example, on an Android or iOS device).
- IT support can install apps and updates on your computer.
- IT support permissions
- When you enroll your device, you are giving IT support permission to:
- Reset your device back to the manufacturer's default settings. This is helpful if the device is lost or stolen.
- Remove work-related files and business apps. Personal data and settings aren't removed.
- See the software installed on the device, including software you've personally installed.
- Set requirements on your device, like requiring you to have a device password or PIN. Your org might also limit how many times you can enter an incorrect password, and might lock you out of the device if you try too many times.
- Require you to encrypt the data on your device to help protect company data, in case your device is lost or stolen.
- Require you to accept terms and conditions.
- Block you from using the device camera or screenshot feature. This restriction limits the sharing of work-related data.
- Device syncing for updates
- Every eight hours, enrolled devices will sync with Intune to get the latest updates and policies from your org. During check-in the device can:
- Download policy or app updates.
- Receive hardware inventory updates.
- Receive app inventory updates.

Links

Company Portal

https://portal.manage.microsoft.com/devices

Overview

https://docs.microsoft.com/en-us/mem/intune/user-help/use-managed-devices-to-get-work-done

What can/can't the IT dept see?

https://docs.microsoft.com/en-us/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

What happens to my computer after enrollment?

https://docs.microsoft.com/en-us/mem/intune/user-help/what-happens-if-you-install-the-company-portal-app-and-enroll-your-device-in-intune-windows?source=recommendations