MGroupServices

BYOD SETUP ON IOS DEVICE

iOS

BYOD INTRODUCTION

Bring Your Own Device (BYOD) facilitates a friendly way to access corporate data on your personal device in a secure way. This approach simply manages the apps that contain corporate data.

Intune protects the corporate data even if the app in question accesses both corporate and personal data for all Microsoft Office mobile apps.

A BYOD policy outlines what the company sees as an acceptable use of the technology, how to operate it and how to protect the company from cyber threats such as ransomware, hacking and data breaches.

If you're accessing any Work resources (such as Outlook, Teams, OneDrive etc.) on your Personal Mobile Phone, MS Office applications are required to have a 6 digit passcode to access the apps protecting the corporate data.
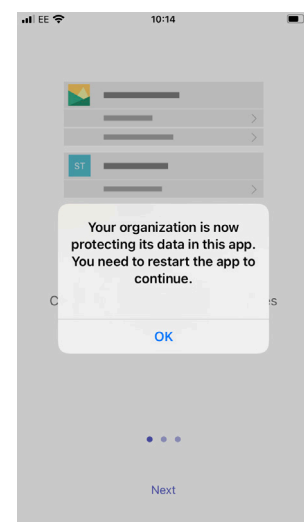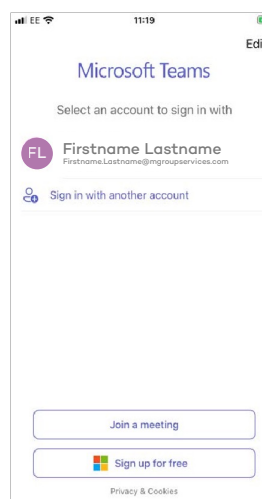
MGroupServices
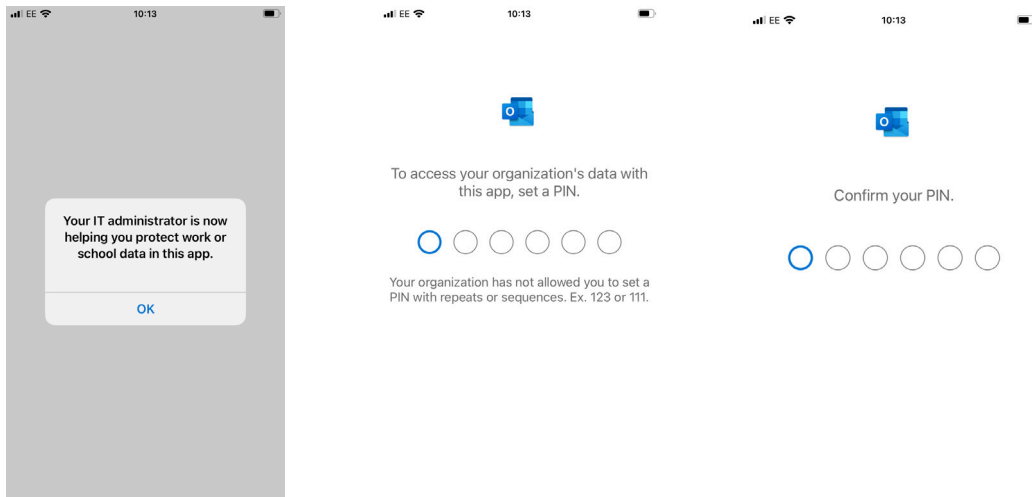
1.

Download and install Teams.
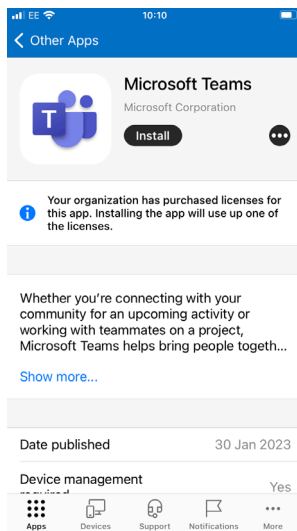
2.

Tap on the application downloaded, complete configuring the app. If it prompts to Authenticate, please follow onscreen instructions to Authenticate your login. App will prompt to restart the app.

MGroup Services

3.

Close and reopen the app, it will prompt the below message. Tap **OK** and setup a passcode for Microsoft Applications.

Your IT administrator is now helping you protect work or school data in this app.

OK

To access your organization's data with this app, set a PIN.

Your organization has not allowed you to set a PIN with repeats or sequences. Ex. 123 or 111.

Confirm your PIN.

NOTE: Remember this passcode is to be used by all Microsoft applications.

Configuration Successfully Completed.