Mobile Device Management Policy

Giles Brook School

GILES BROOK SCHOOL

Written by:	Jenny Brown	**Date:** 11/04/2018
Last reviewed on:	18/03/2020	
Next review due by:	11/04/2021	

This policy is to explain how the school protects school data and personal information on staff personal mobile devices. To help with communication within school, staff may find it beneficial to have Google Mail and Google Drive on a personal device example smart phone. Phones in their nature are at most risk of being lost or stolen, It is therefore imperative that the school maintains control of school data.

If you wish to use your personal device to access Google Drive and Google Mail, then you will have to accept certain school policy procedures for your personal device. There is no flexibility with this, it will be either the school policy or not at all. You are able to access mail and drive on your school iPad which has to have the school policy in place.

If your device is lost or stolen the headteacher must be notified straight away, so that the IT technician can be informed to block the Google account on your personal device. This data/information is recoverable if/when the device gets found.

iPhone:

1. When you first try to login, it asks to install a Security Certificate (this has been renewed for apple devices, 10th April 2019) - It will force you to install the security certificate.
2. Passcode requirement is an **8 character password** letter / number / special character - it will force you to update your password
3. Device Policy Alert - Admin must approve the device and an Email is sent to IT Technician.
4. Your phone will now be visible in the Google Admin Panel
5. Once complete it will allow the administrator to **BLOCK** i.e. remove the users Google account from the device; when they try to logon tell them they are blocked. Basically it un-approves the device.
6. It is also possible for the administrator to **WIPE DEVICE** - this would not be our policy to do so unless the user requested us to do so on their behalf. The request will have to be made in writing.
7. We will not change any other settings on the device.

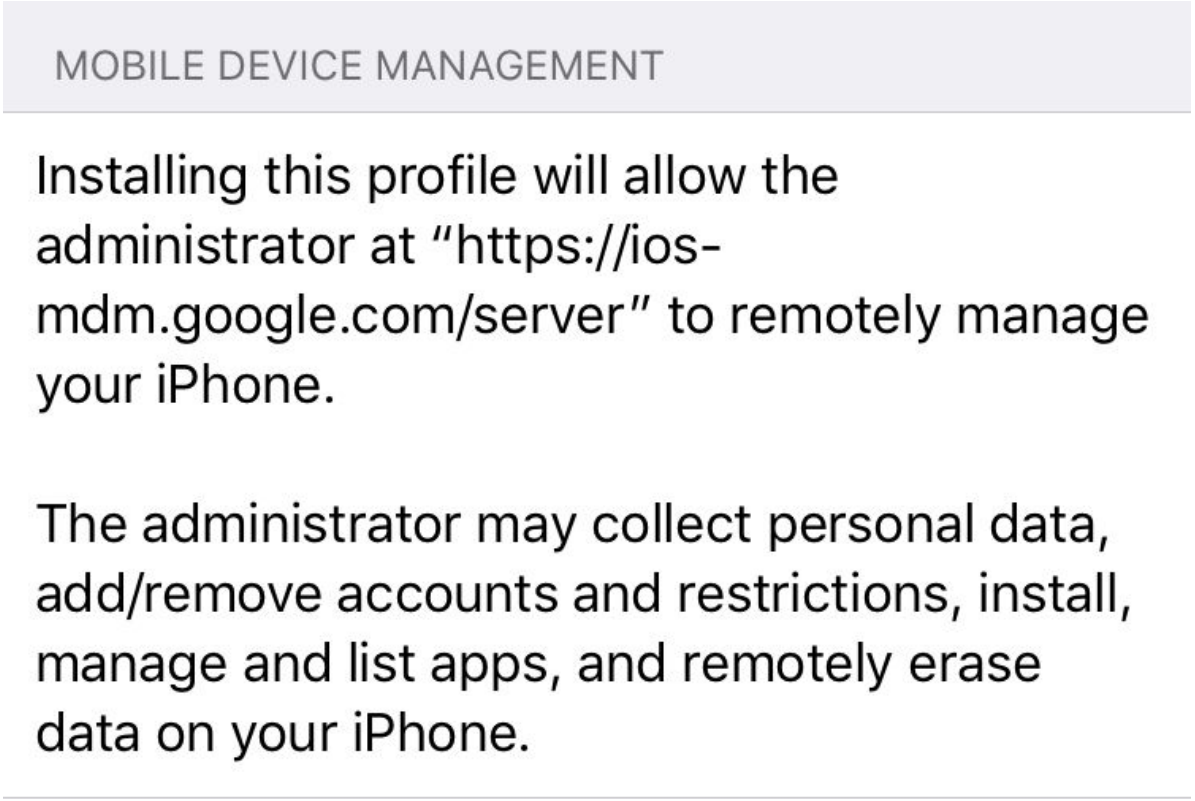
Android:

1. When you first try to login, it asks to install a Security Certificate. It will force you to install the security certificate.
2. Passcode requirement is an **8 character password** letter / number / special character - it will force you to update your password
3. Device Policy Alert - Admin must approve the device and an Email is sent to IT Technician.
4. Your phone will now be visible in the Google Admin Panel
5. Once complete it will allow the administrator to **BLOCK** i.e. remove the users Google account from the device; when they try to logon tell them they are blocked. Basically it un-approves the device.
6. It is also possible for the administrator to **WIPE DEVICE** - this would not be our policy to do so unless the user requested us to do so on their behalf. The request will have to be made in writing.
7. We will not change any other settings on the device.

Rules for ALL users Mobile Devices

1 Tapestry **MUST NOT** be installed on a Personal Device.
2. You are **NOT** allowed to add the schools Gmail account to Apple mail or any other POP or IMAP mail app.
3. You are not allowed to access Gmail or Google Drive through any other browser except Google Chrome.

When you login to Google from a personal device, you will get this message:



Personal Data that is collected is:

Device ID:

Serial Number:
First Sync:
Last Sync:

It only controls Google APPS on your personal device. We would not remove access to any Google app from the device. It doesn't show any other apps you access. No personal data is available. It's purely to control Google and to give the control to the school to remove the school account.

If you would like to see exactly what information is collected before you enrol then see Jenny Brown.