Using a personal device to connect to the corporate email system

This policy outlines procedures for accessing corporate information on personally owned devices.

Definitions

A device is defined as, but not limited to, the following: Smartphone, Tablet, Laptop.

General Principals

In certain cases, where your specific role and responsibilities deem it appropriate, and subject to approval, you may be issued with a Company phone. This is for exclusive use on Company business and will be set up according to the protocol outlined in this policy.

Where there is no business reason for you to have a Company phone, which will be the case for most employees, you may still wish to use your personal device to access Company information, for example work emails.

In this case, both yourself and Kings are required under the terms of GDPR to secure personal data according to the protocol set out in this policy.

In order for Kings to protect personal information, personal devices will need to be registered with the Corporate Mobile Device Management platform (MDM). This will enable Kings to remove any corporate information when your employment with Kings ceases.

Conditions of use

Once your device has been enrolled in the MDM system you will:

- Be able to access corporate email/calendar/contacts using the Microsoft Outlook App.
- Be able to access corporate documents stored in OneDrive using the Microsoft OneDrive App.

The use of any other applications or apps to access email and documents is not permitted and will be monitored.

Once your device has been enrolled in the MDM system a Management application will be installed and Kings:

May have access to:

- Make/Model and serial number of device.
- Operating system.
- App Names.
- Owner and device name.

Will not see:

- Call and web history.
- Email and text messages.

- Contacts and calendar.
- Passwords.
- Photos.

You should ensure that:

- No other users have access to your device to see corporate information.
- You have a regular backup of your device contents.
- The DPO is notified immediately upon the loss or theft of your device, so that, if necessary the ICO can be notified.

Your device will not connect if:

- You do not use a strong password/passcode.
- Your device is not encrypted.
- Your device is jailbroken/rooted or modified.

When your employment with Kings ceases a "selective" wipe will be performed on your device. This will remove all Company data (emails and documents) and remove your device from the MDM. It is possible, although extremely unlikely that your device could be "wiped to factory defaults".

It is preferable to remove corporate information in person on your last day of employment (once you confirm that you have a recent backup) although if this is not possible then the "selective wipe" can be performed remotely.

I wish to access corporate information on my personal device and I agree to the terms of this policy.

Employee

Date: ……..

Name: ……

Signature: ……..