



## **Mobile Equipment Security Policy**

A mobile working policy is in force that requires mobile devices (including BYOD-Bring Your Own Device) to be kept up to date with vendor updates and application patches.

**Mobile Use Policy – Corporate** – a mobile smart phone is provided by the company.

- This device can be used for personal, legal use under a discretionary fair use as decided by the company. If personal usage is deemed too high a warning will be given and may lead to a disciplinary. It is the user's responsibility to keep the phone and the data on the phone secure to the best of their abilities any breach due to user negligence may again result in a disciplinary.
- It is the user's responsibility to ensure all updates to any other company approved installed app are applied when notification is given of an update.
- It is the user's responsibility to back up any personal information on the mobile device.
- It is the user's responsibility to report any suspected security issue on the phone.
- It is the user's responsibility to report any loss or theft of the phone immediately.
- The company can remotely lock or wipe the mobile device at any time.
- The mobile device remains the property of the company.
- No social media activity to be undertaken on the company mobile without written approval from the company.

This policy will be reviewed annually, in line with other IT policies and procedures.

## **Mobile Use Policy – BYOD (Bring Your Own Device)**

- Users are allowed to install corporate apps and accounts on their personal device only under the following condition: Written approval from the IT manager.
- The device must have a pin code or password to unlock.
- The user must report any loss or theft of the phone immediately.
- It is the device owners' responsibility to maintain a backup of data and the company is not liable for the loss of any data on the device.
- The company does not support the user of any company data on any device that is not owned by the company. Having any corporate data on a personal device is not permitted.

This policy will be reviewed annually, in line with other IT policies and procedures.

A handwritten signature in blue ink, appearing to read 'A. King', is positioned above the printed name of the Managing Director.

Managing Director  
January 2019